KDT900
Kiosk Data Terminal

User's Guide

Effective date: **October 2009**

Revision History

October 1, 2009 – Initial version

American Microsystems, Ltd.
2190 Regal Parkway • Euless, TX 76040
Phone 800.648.4452 • Fax 817.685.6232
www.amltd.com

Table of Contents

About This Document

Introduction	1
What to Expect	1
Chapter Descriptions	1

Chapter 1 – Introduction

Introducing the KDT900	1-2
Part Numbers and Model Information	1-2
Warranty Information	1-3
Agency Compliance	1-3

Chapter 2 – Getting Started

KDT900 Startup Sequence	2-2

Chapter 3 – Terminal Overview

Outer Case Description	3-2
Rear Panel Description	3-4
Opening the KDT900 Outer Case	3-5
Internal Connections	3-6
Internal Connector Pinouts	3-6
External Connections	3-9
Wiring Installation	3-9
Power Requirements and Battery Information	3-10
Main Power Switch and Power-On Reset	3-12
Secure Digital (SD) Card	3-12

Chapter 4 – Communications

Serial Communications	4-2
USB Communications (Host)	4-2
USB Communications (Slave)	4-2
Digital I/O	4-3
Weigand Interface	4-5

Chapter 5 – Wireless Networking

Overview	5-2
802.11 Fallback	5-2
Interference and Coexistence	5-3
Encryption and Authorization	5-3
Wireless Configuration	5-3

Chapter 6 – Integrated Bar Code Scanner

Overview 6-2
Determining Scanner Type 6-2
Linear CCD Aiming System and Decode Zones 6-3
2D Omni Scanner Aiming System and Decode Zones 6-3
Triggering the Scanner 6-5
Scanning Bar Codes 6-5
Supported Bar Code Symbologies 6-6
Obtaining and Using Scan Engine Setup Bar Codes 6-7

Chapter 7 – Windows® Embedded CE 6.0

General Usage 7-2
Calibrating the Touchscreen 7-3
Connecting to a PC 7-5
Programming the Pushbuttons 7-6
Changing the MSR and Barcode Reader Settings 7-8
Persistent Storage 7-9
Preinstalled Software 7-9

Chapter 8 – Mechanical Integration & Mounting

Rear Panel Mount Points 8-2
Flush Wall Mounting 8-3
Angled Wall Mounting 8-4
Column/Post Mounting 8-5
RAM Mounts 8-6

Appendix A – Technical Specifications
Appendix B – Wireless Reference Table

About this Document

Introduction

This document describes the integration and general use of the AML KDT900 kiosk data terminal.

This document is provided as **PRELIMINARY ONLY** and is not intended as a complete product reference. AML reserves the right to make changes to this document and to any hardware, software or product it describes.

What to Expect

This user's guide provides an overall physical description, built-in hardware functions, technical specifications and performance capabilities of the KDT900 terminal. In addition you will learn how to:

- Open the tamper resistant case
- Connect communication cables
- Cold boot and warm reset the KDT900
- Navigate the KDT900 software
- Mount the unit using optional accessories

Chapter Descriptions

Chapter 1 – gives a brief overview of the KDT900, its product warranty and agency compliance

Chapter 2 – gives a quick start introduction to the KDT900 unit

Chapter 3 – describes the KDT900 terminal hardware and details internal and external cable connections

Chapter 4 – describes the communication and user input capabilities of the KDT900

Chapter 5 – describes the use and configuration of the optional 802.11 wireless LAN radio

Chapter 6 – describes the use of the optional internal bar code scanner

Chapter 7 – Windows® Embedded CE 6.0

Chapter 8 – describes methods to mount the KDT900 unit in a variety of environments

1

Introduction

This chapter gives a brief overview of the KDT900, it's product warranty and agency compliance.

Introducing the KDT900

The KDT900 is an industrially rated, kiosk-style data terminal designed for use in retail price checking, retail data collection, real-time work-in-process, industrial data collection, consumer lookup and time and attendance.

The terminal is designed around a 5.6" Full VGA, high-color LCD with integrated touchscreen that provides an unsurpassed viewing experience. The ultra-bright LED backlight allows for viewing images and text on the screen in even the brightest of environments.

The KDT900 is designed to be connected to multiple external and internal data sources including bar code scanners, magnetic stripe readers, keyboards, proximity card readers and other modern information collection devices. Its primary wide area communication is through an integrated Power-over-Ethernet ready 10/100 BaseTX Ethernet port or an optional 802.11b/g/n radio.

With a dual port digital I/O and 3 full-speed USB host ports, the KDT900 can be adapted into any environment and provides a cost-effective solution for any number of industrial and consumer installations.

Part Numbers and Model Information

Model Number	Bar Code Scanner	Wired Networking	Wireless Networking	Backup Battery	Power-over-Ethernet
KDT900-0000	n/a	10/100 BaseTX	n/a	n/a	802.3af
KDT900-0001	CCD	10/100 BaseTX	n/a	n/a	802.3af
KDT900-0002	2D	10/100 BaseTX	n/a	n/a	802.3af
KDT900-0003	1D Laser	10/100 BaseTX	n/a	n/a	802.3af
KDT900-0004	Ext. Omni	10/100 BaseTX	n/a	n/a	802.3af
KDT900-0010	n/a	10/100 BaseTX	802.11b/g	n/a	802.3af
KDT900-0011	CCD	10/100 BaseTX	802.11b/g	n/a	802.3af
KDT900-0012	2D	10/100 BaseTX	802.11b/g	n/a	802.3af
KDT900-0013	1D Laser	10/100 BaseTX	802.11b/g	n/a	802.3af
KDT900-0014	Ext. Omni	10/100 BaseTX	802.11b/g	n/a	802.3af
KDT900-0100	n/a	10/100 BaseTX	n/a	2200 mAh	802.3af
KDT900-0101	CCD	10/100 BaseTX	n/a	2200 mAh	802.3af
KDT900-0102	2D	10/100 BaseTX	n/a	2200 mAh	802.3af
KDT900-0103	1D Laser	10/100 BaseTX	n/a	2200 mAh	802.3af
KDT900-0104	Ext. Omni	10/100 BaseTX	n/a	2200 mAh	802.3af
KDT900-0110	n/a	10/100 BaseTX	802.11b/g	2200 mAh	802.3af
KDT900-0111	CCD	10/100 BaseTX	802.11b/g	2200 mAh	802.3af
KDT900-0112	2D	10/100 BaseTX	802.11b/g	2200 mAh	802.3af
KDT900-0113	1D Laser	10/100 BaseTX	802.11b/g	2200 mAh	802.3af
KDT900-0114	Ext. Omni	10/100 BaseTX	802.11b/g	2200 mAh	802.3af

CCD = Linear Imager
2D = Omni-directional Imager with 2-Dimensional decoding
1D Laser = Integrated 1D Laser
Ext. Omni = External Omni-directional Laser

Part Number	Description
ACC-0750	KDT750/900 Pole/Post Mount Kit
ACC-0752	KDT750/900 Angled Wall Mount Kit
ACC-0754	KDT750/900 Ram Mount Kit
ACC-750MSR	KDT750/900 Magnetic Stripe Reader Kit (Top Mount)
ACC-750HID	KDT750/900 HID ProxPoint Plus Reader Kit (Side Mount)

Warranty Information

A one-year warranty against material defects and workmanship from the date of shipment is guaranteed by AML. Products are sold on the basis of specifications applicable at the time of manufacture. AML shall have no obligation to modify or update products once sold. At our option, we will repair or replace, at no charge, any unit that proves to be defective providing the appropriate steps are taken to procure an RMA (Return Materials Authorization) number and shipping instructions from AML.

Agency Compliance

FCC Declaration of Conformity
Product Name: Model KDT900 Kiosk Data Terminal
Model Number: KDT900

This equipment complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This equipment may not cause harmful interference, and (2) this equipment must accept any interference received, including interference that may cause undesirable operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If you determine the equipment does cause harmful interference to radio or television reception (this may be determined by monitoring the interference while turning the equipment off and on), you are encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or TV technician for help.

2

Getting Started

This chapter gives a quick start introduction to using the KDT900.

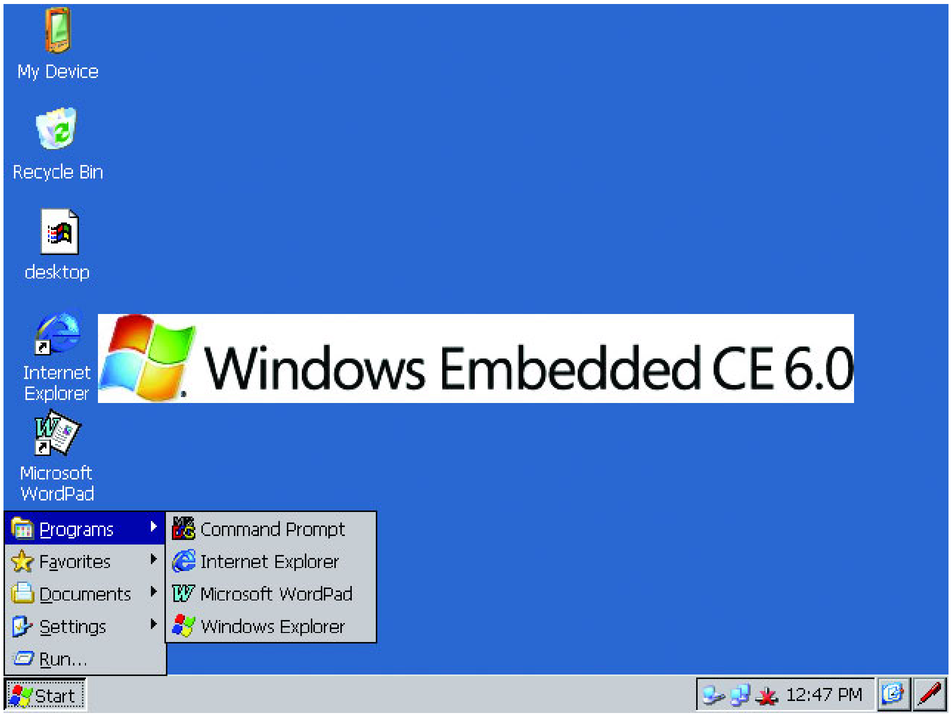
KDT900 Startup Sequence

The KDT900 unit will begin booting the operating system once power is applied to the terminal and the rear panel is completely closed.

NOTE: The rear panel must be in place before the unit will power up.

Once powered on, the KDT900 will automatically start the Windows® Embedded CE 6.0 operating system.

When the unit is done booting, the Windows Desktop screen will be displayed.



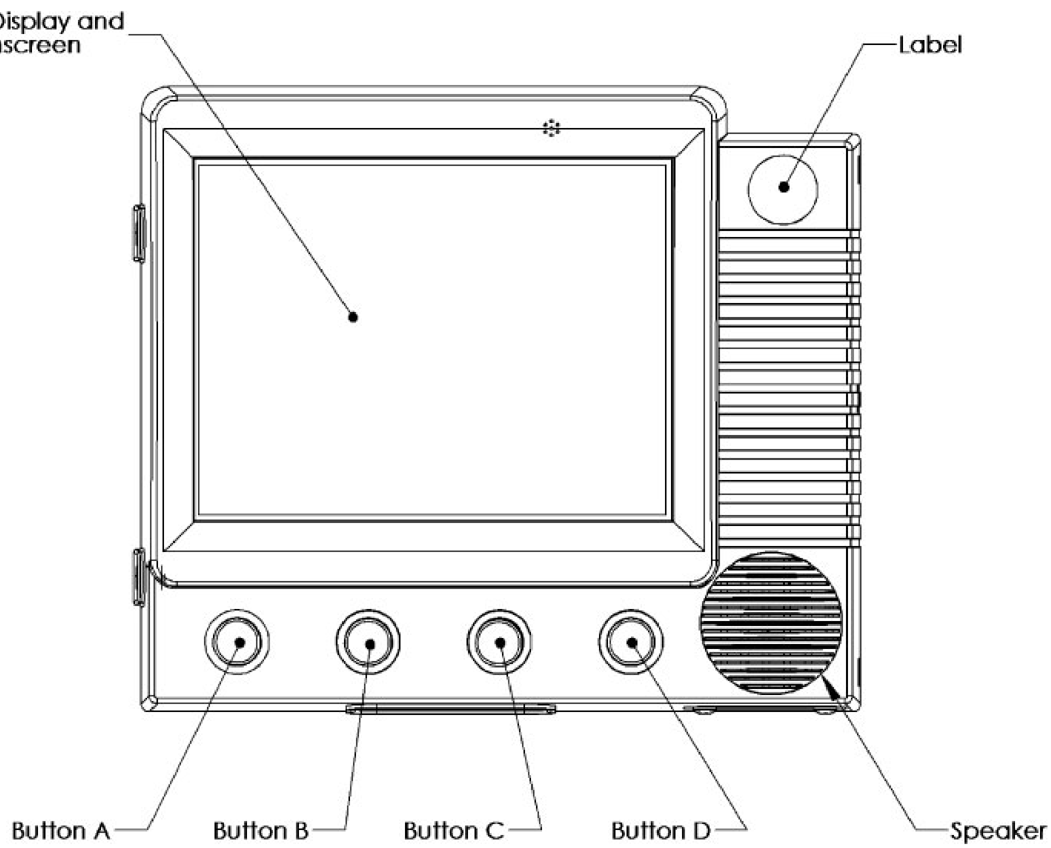
Many of the Windows setting can be controlled under the Control Panel. See the Wireless Networking chapter for instructions on setting the optional wireless network.

3

Terminal Overview

This chapter describes the KDT900 terminal hardware and details internal and external cable connections.

Outer Case Description



LCD Display and Touchscreen

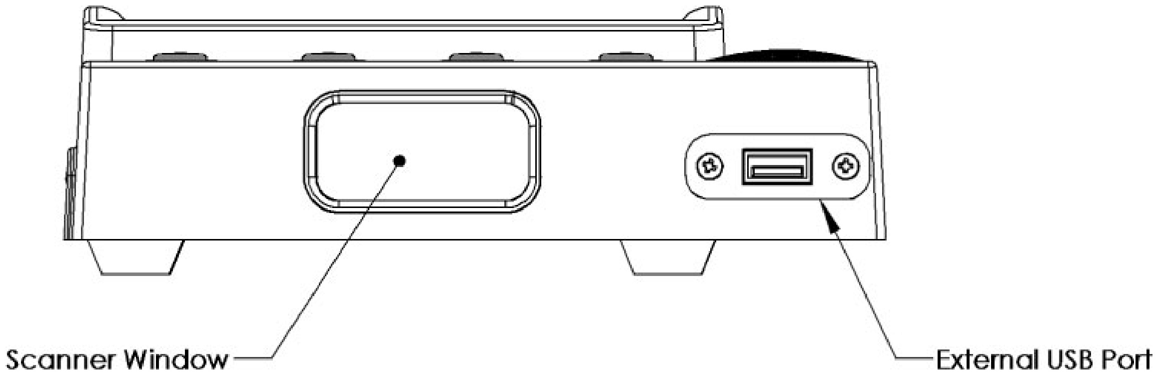
The unit features a 5.6" Full VGA (640x480 pixels) color display with an ultra-bright backlight for an unsurpassed level of viewability. The LCD is bonded to an industrial rated, resistive touch panel for user input.

Buttons A, B, C, D

The device has four programmable, momentary pushbutton type switches on the front case that can be used for special features or user input.

Speaker

A 1.5 inch, half-watt internal speaker is available for programmable tonal user feedback.

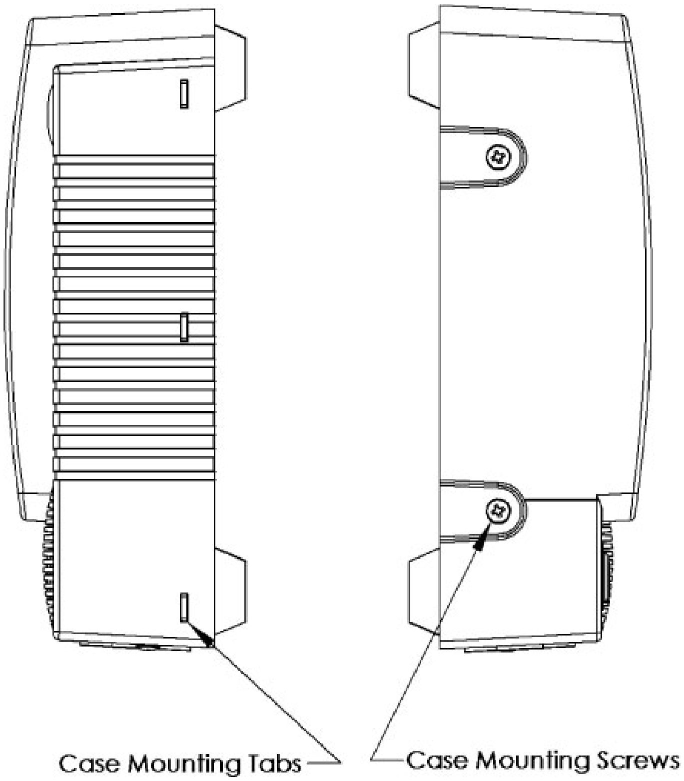


Scanner Window

The KDT900 is available with one of many integrated bar code scanner options including a Linear CCD Imager, 1D Laser or 2D Imager for decoding bar codes presented under the unit. The decoder's illumination lights will shine through the scanner window at all times. The clear protective lens should be kept clean and free of fingerprints and grime. An optional, externally-mounted Omni-directional Laser is also available.

External USB Port

A diagnostic/administration USB port is available on the bottom of the unit to the right of the scanner window. This port can be disabled internally.



Case Mounting Tabs & Case Mounting Screws

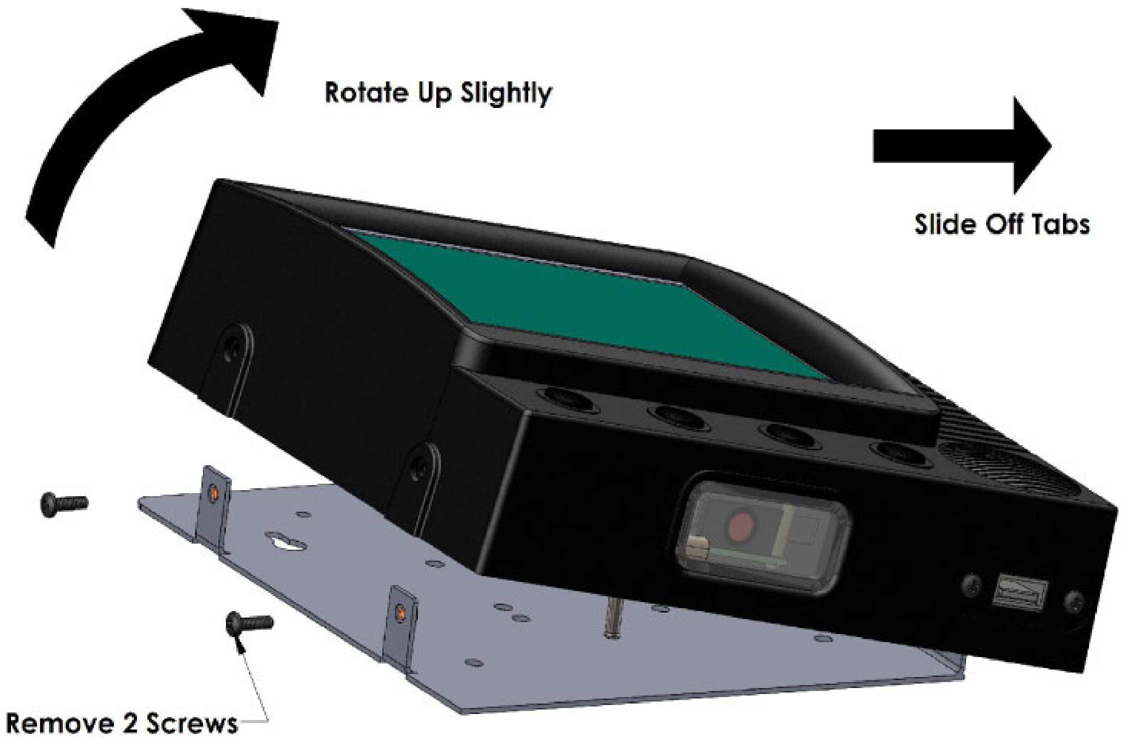
The KDT900 main outer case is held closed on the left side by two #4-40 x 1/4" screws. Longer screws should not be used, as damage to the internal components of the KDT900 can result. The right side of the outer case contains three slots that the matching tabs of the rear panel should slide into.

Rear Panel Description

The rear panel of the unit is made from high quality 1/16" stainless steel. The panel secures the internal connections, seals the unit from dust and debris, and prevents vandalism and unauthorized access.

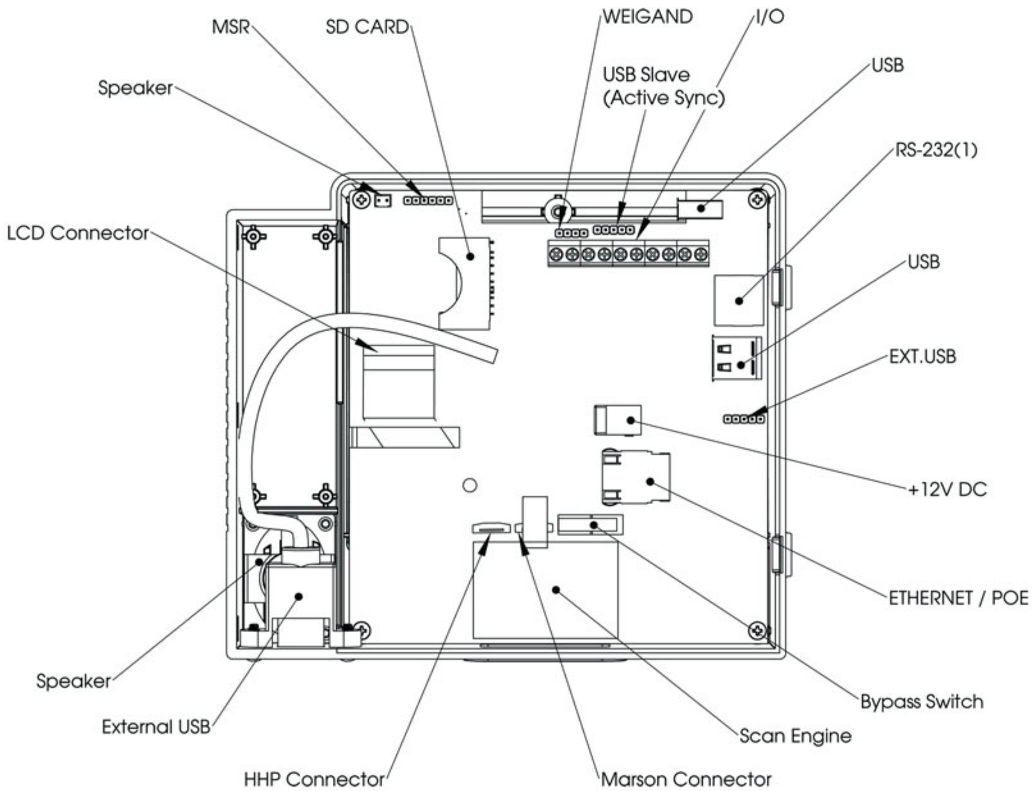
Opening the KDT900 Outer Case

In order to open the KDT900, remove the two screws on the left side and slightly rotate the outer case to the right. Once the unit is opened approximately one inch, the outer case can be slid off of the mounting tabs. All mounting brackets will remain with the rear panel, and the electronics and wiring will stay attached to the outer case.



Internal Connections

Connections to the KDT900 unit are housed internally to prevent vandalism and to secure the device.



Internal Connector Pinouts

Weigand (J3 – 4 Pin Male Header)

Pin	Description	I/O
1	Ground	
2	Data 0	I
3	Data 1	
4	+5V (Max. 0.5A)	I

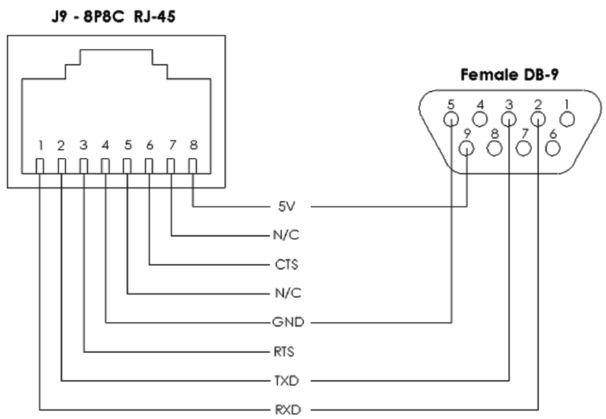
MSR (JP1 – 6 Pin Male Header)

Pin	Description	I/O
1	Ground	
2	Loop to Pin 4	I
3	RXD	I
4	Loop to Pin 2	O
5	TXD	O
6	+5V (Max. 0.5A)	

RS-232 (J9 8 - Pin RJ45)

Pin	Description	I/O
1	RXD	I
2	TXD	O
3	CTS	O
4	Ground	
5	N/C	
6	RTS	I
7	N/C	
8	+5V (Max. 0.5A)	

RJ-45 to DB9 Wiring Diagram



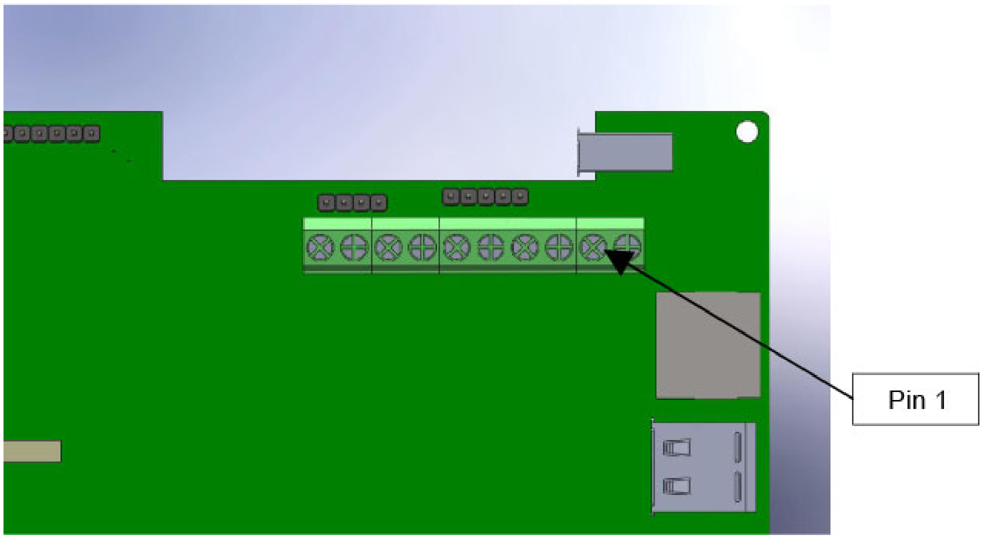
External USB Cable (JP2 - 5 Pin Male Header)

Pin	Description	I/O
1	+5V (Max. 0.5A)	
2	D-	I/O
3	D+	I/O
4	Ground	
5	Shield	

USB Slave (J300 - 5 Pin Male Header)

Pin	Description	I/O
1	+5V (Max. 0.5A)	
2	D-	I/O
3	D+	I/O
4	Ground	
5	Shield	

Digital I/O (J14-J17 - Screw Terminal Block)



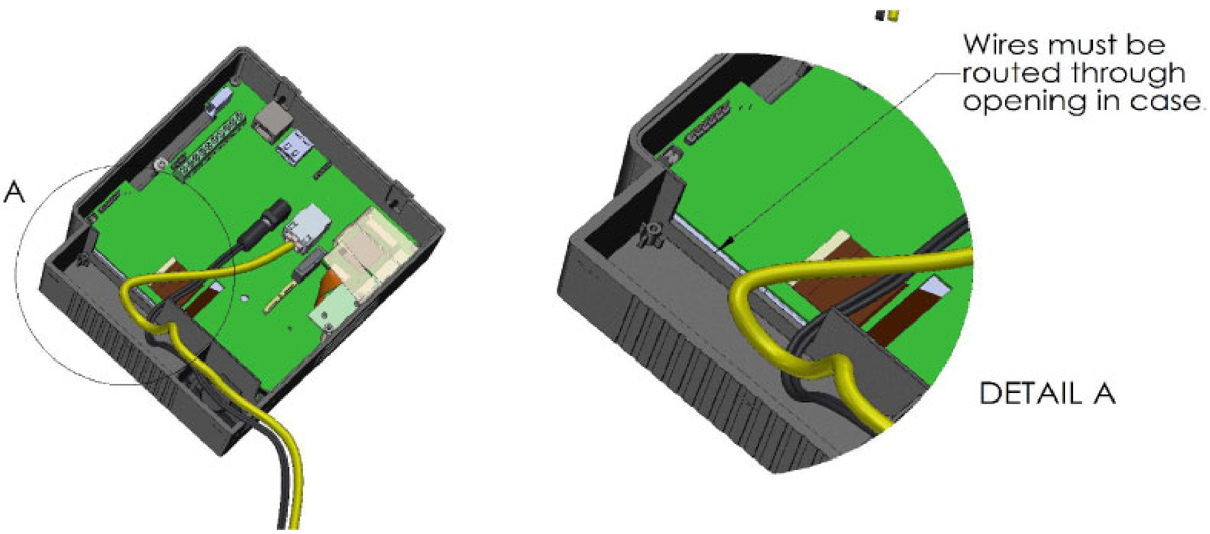
Device	Pin	Description
Relay 1	1	Contact
	2	Normally Closed
	3	Normally Open
Relay 2	4	Contact
	5	Normally Closed
	6	Normally Open
Input 1	7	High/Low
	8	Low/High
Input 2	9	High/Low
	10	Low/High

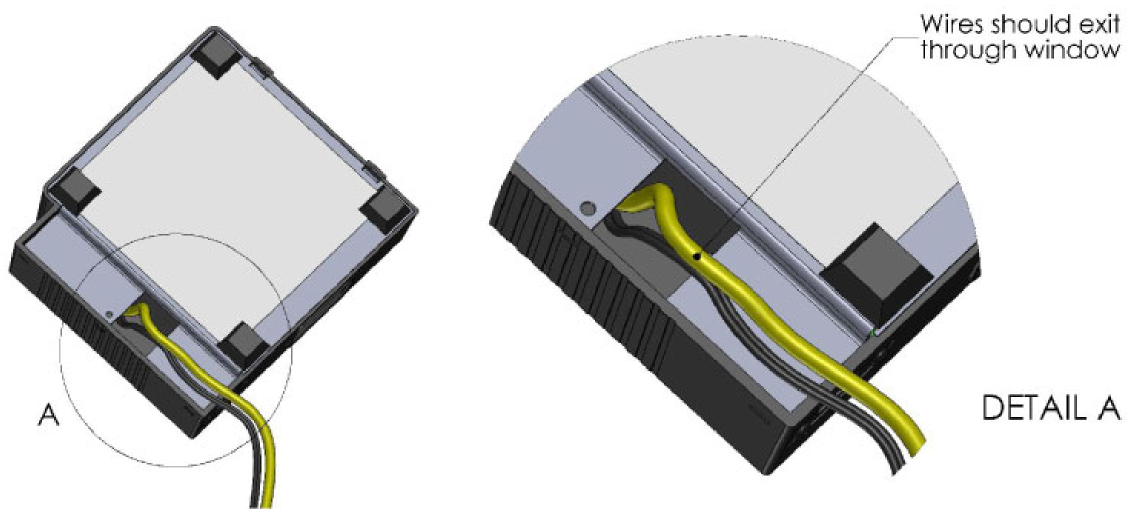
External Connections

The KDT900 houses a single external USB host port. In high security installations, this port can be disabled by disconnecting the internal cable from the port header.

Wiring Installation

To prevent vandalism and unauthorized use, all major connections to the KDT900 base unit are internally housed. All wires exiting the base unit should be routed into the recessed channel, through the opening of the divider wall in the case. The cables should then exit the rear panel through the window at the bottom of the channel.





Power Requirements and Battery Information

The KDT900 can utilize three power sources: external DC power supply, Power-over-Ethernet and an optional internal backup battery.

External DC Power Supply

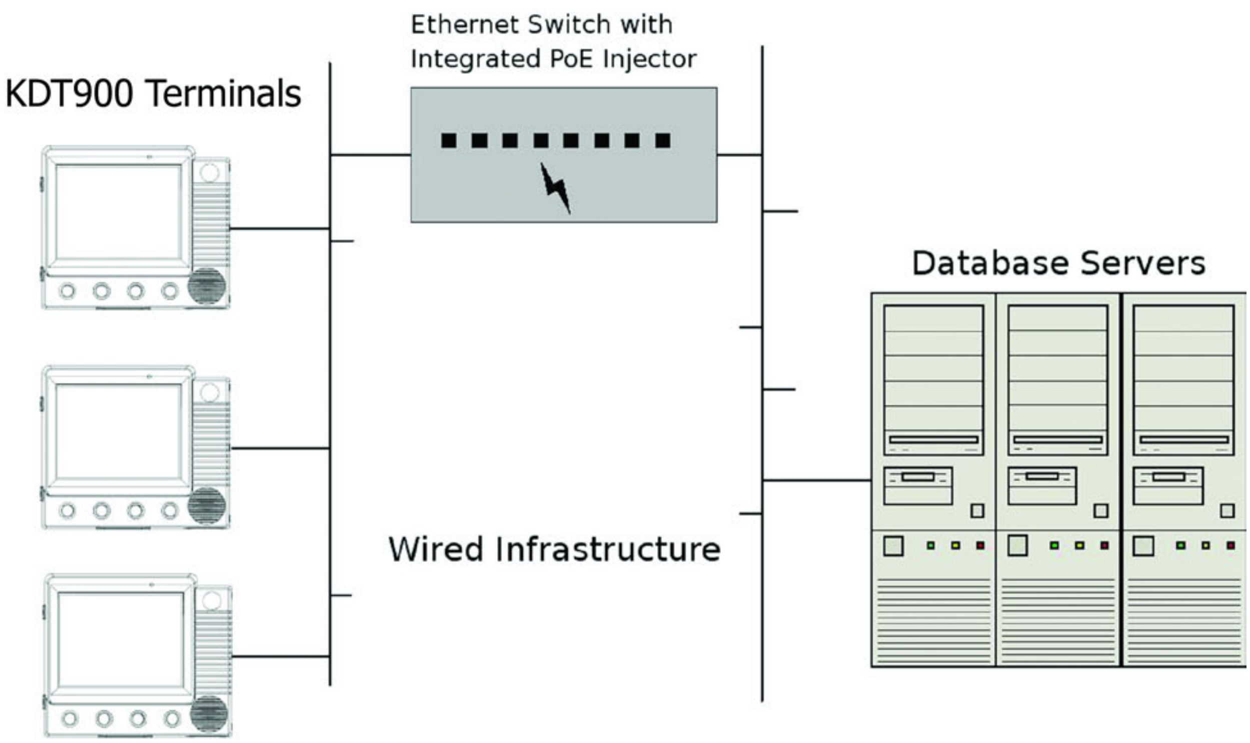
NOTE: Using power supplies that are not approved by AML for use with the KDT900 unit can cause damage to the unit and will void all warranties.

Voltage	12V, regulated
Current	1.5A
Connector	2.1mm Barrel, center positive

Internal Power-over-Ethernet Supply

The KDT900 contains a 802.3af compatible power supply. The unit can be powered via category 5 networking cable when used with an 802.3af compatible power injector. Both network data traffic and power can be sent via the same category 5 wire.

Standard	IEEE 802.3af
Class	0 (12.94 Watts)



Optional Backup Battery

If the KDT900 unit is equipped with an optional internal backup battery, the unit will continue to operate when all other power sources are lost. Depending on the configuration and usage, the backup battery should enable the unit to operate for approximately one hour.

When power is applied to the unit, the backup battery will be automatically charged. After a complete discharge, the backup battery should be charged 48 hours before use.

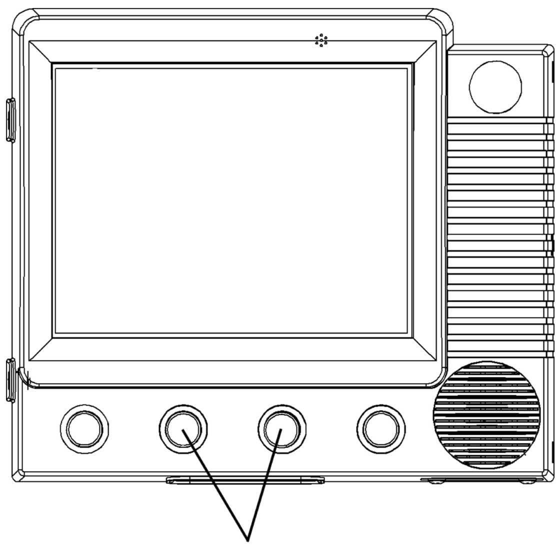
NOTE: The backup battery is permanently connected to the KDT900 motherboard. Do not attempt to remove the battery. The KDT900 unit must be properly disposed of and the battery recycled when it has reached the end of its usable life.

Type	2 Cell, Li-ion
Voltage	7.4V
Capacity	2200mAh

Main Power Switch and Power-On Reset

The KDT900 unit contains a main power switch that disables the unit when the rear panel is removed during servicing and installation. This switch is designed as a safety measure, and it is not recommended that the switch be bypassed or modified in any way.

To reset the KDT900 unit with power enabled, hold down the middle two pushbuttons for 10 seconds or until the LCD screen goes black. When the buttons are released, the unit will perform a warm boot.



Secure Digital (SD) Card

The internal SD card is required for normal operation of the KDT900 unit. The card can be removed and connected to a PC for configuration, upgrades and file transfer, but the device should not be powered on without it properly installed and secured.

All KDT900 configuration files are located on the SD card.

4

Communications

This chapter describes the communication capabilities of the KDT900.

Serial Communications

The KDT900 contains two user accessible RS-232 ports and one bar code scanner port for serial communications with a PC or other peripheral devices. Each port is capable of baud rates up to 115.2 Kbps.

Serial communication ports are used to communicate with devices such as:

- Internal Bar Code Scanner
- External Bar Code Scanner
- External Magnetic Stripe Reader
- Serial Printer
- PC

The serial.settings file is used to configure the three RS-232 serial ports on the KDT900. Each port is designed for a specific function and may or may not be used depending on the KDT900's hardware configuration.

USB Communications (Host Ports)

The unit contains three user accessible USB 1.1 Full speed host ports, capable of data rates up to 12 Mbps.

Common USB devices that can be used with the KDT900 are:

- External Bar Code Scanner
- External Magnetic Stripe Reader
- External Keyboard
- USB storage devices ("thumb" or "pen" drives)

No configuration is necessary for USB devices that are compatible with the KDT900.

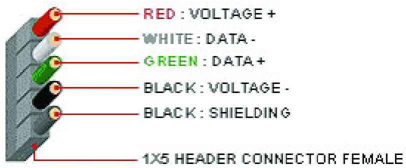
USB Communication (Slave Port)

The KDT900 has one USB Slave Port for communicating to a PC via Microsoft® ActiveSync® and Windows® Mobile Device Center.

This port can be used for file transfer, application installation and firmware upgrades.

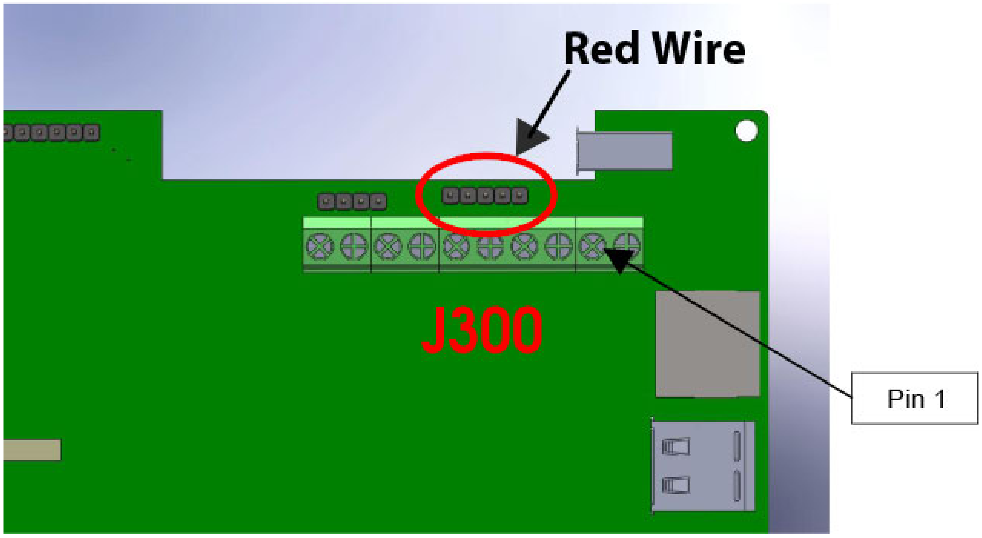
Cable Requirement

The KDT900 requires a USB Slave adapter cable to connect to a PC. This cable has a five pin connector on one end and a standard USB Type-A connector on the other:



Internal Connection

The cable is connected to the internal connector of the KDT900 motherboard labeled **"USB SLAVE"** or **"J300"**. *The RED wire of the cable MUST BE CONNECTED TO THE RIGHTMOST PIN!*



Digital I/O

The KDT900 base unit contains two electrically isolated digital inputs and two electrically isolated digital outputs.

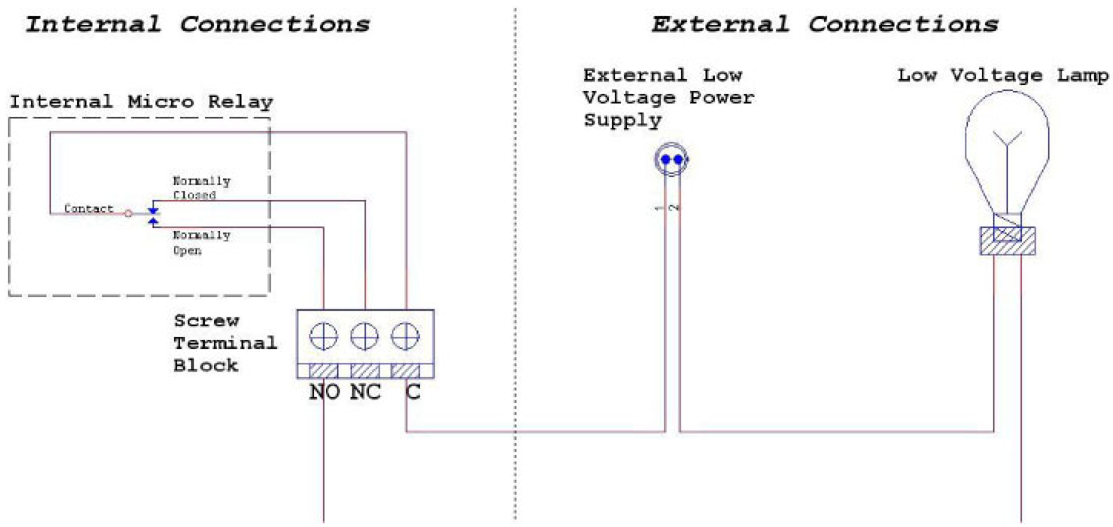
Digital Outputs (Micro-Relays)

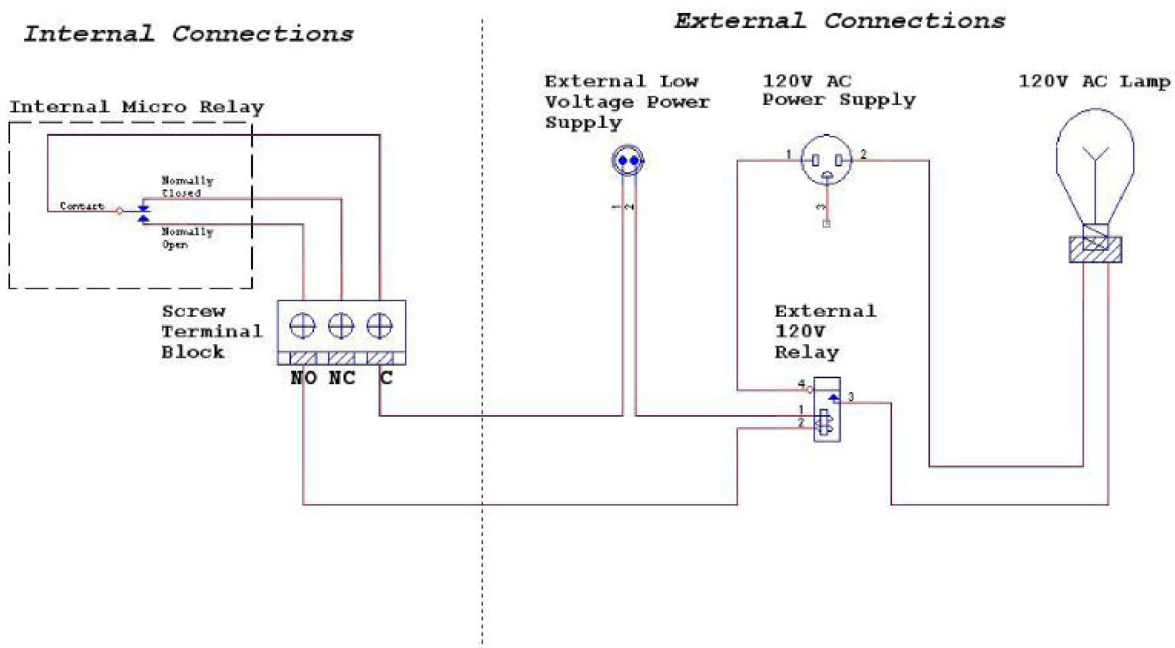
The KDT900 digital outputs are controlled via internal micro-relays driven by the microprocessor. These relays can be used to drive external devices such as:

- Lights and Beacons
- Door Strikers
- Sirens
- Stationary Scanners

The internal relays are designed for low voltage applications. To use the relays in high voltage situations, an additional external relay should be implemented.

Relay Wiring Diagrams



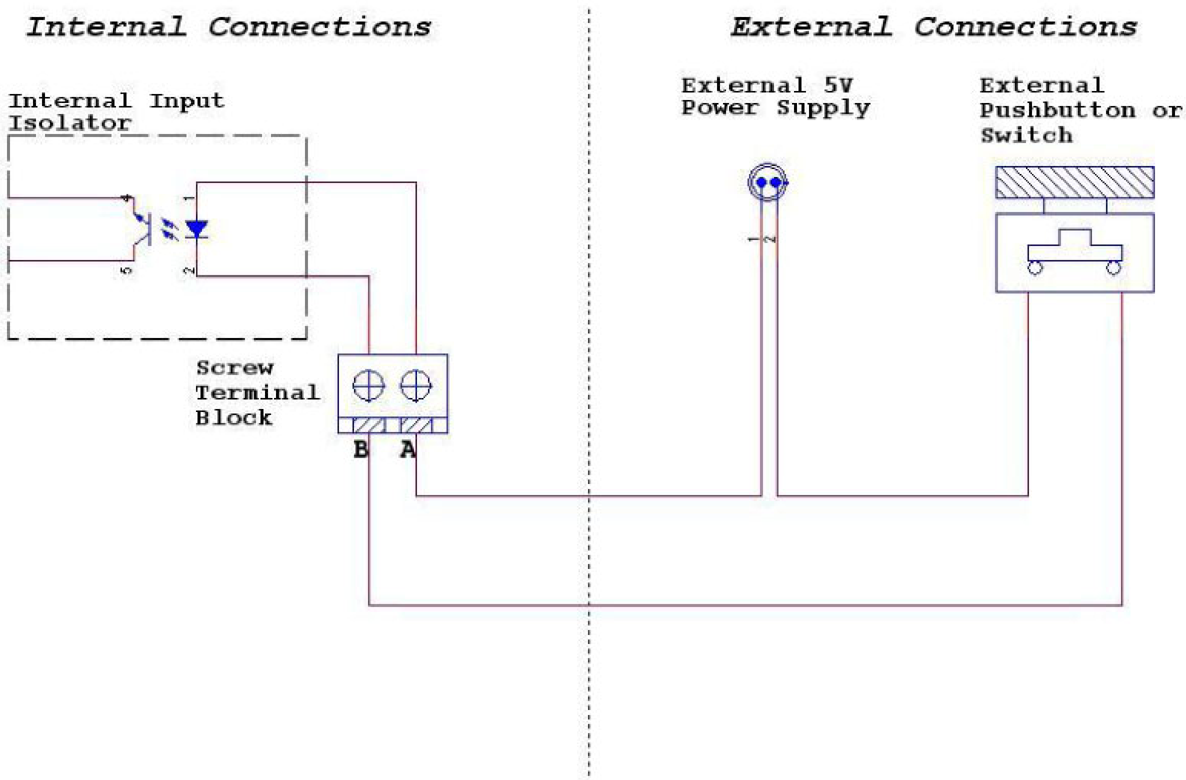


Digital Inputs (Opto-Isolators)

The KDT900's internal digital inputs can be used to signal events and actions from an external source. Possible uses for the isolated input are:

- External Pushbutton Switches
- Door Sensors
- Proximity Sensors

Digital Input Wiring Diagram



Weigand Interface

The Weigand interface is used to connect proximity card and smart card readers to the KDT900. Weigand is a simple, two-wire interface used to transmit uni-directional data from a peripheral device to a host.

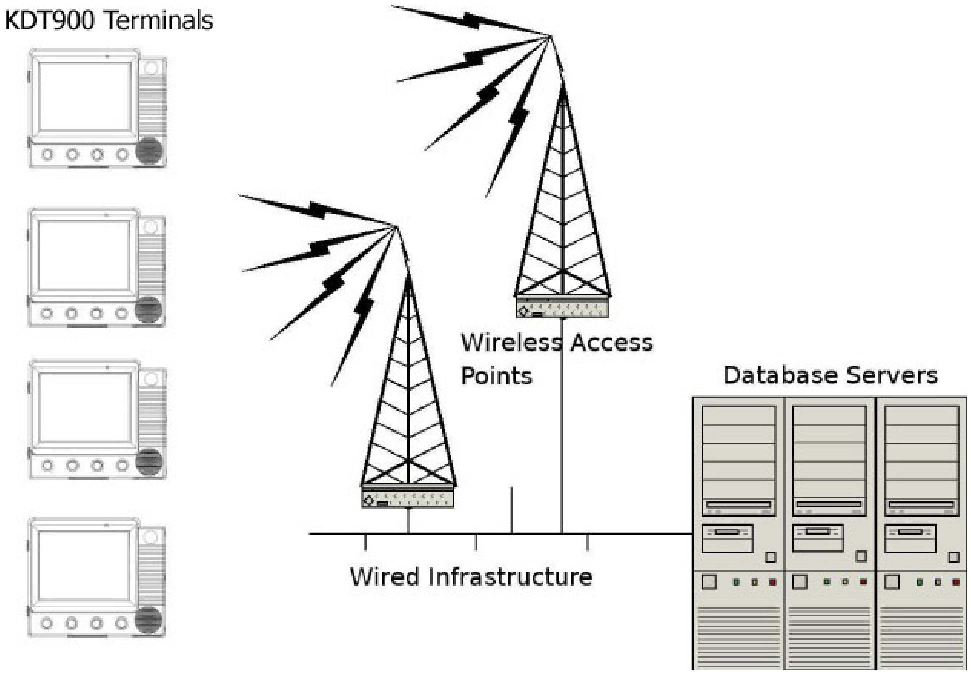
5

Wireless Networking

This chapter describes the configuration of the optional internal 802.11 radio.

Overview

The KDT900 terminal can contain an optional 802.11b/g/n radio and internal antenna. This radio is specifically designed to communicate with any 802.11b/g or 802.11n (Draft v2.0) Access Point.



The range of the radio depends greatly on the quality of the Access Point and the RF communications characteristic of the environment where the device is used. The typical range for an 802.11 radio is 300 feet through free air. Additional Access Points must be added to improve coverage in a larger area, or in electrically noisy RF environments.

802.11 Fallback

Wireless LAN technology is designed to make maintaining a connection between two devices as reliable and consistent as possible. Since the speed of the connection between wireless devices will vary as range and signal quality varies, the wireless devices will intentionally sacrifice throughput (data rate or connection speed as measured in bits per second) in exchange for maintaining a reliable connection. In other words, a reliable connection at a lower speed is preferred over an unreliable connection at a higher speed (i.e., it is easier to maintain the connection if data rate is deliberately reduced, or put another way, lower data rates will tolerate a higher range and/or worse signal quality). This characteristic is known as fallback. As example, an 802.11b system will fallback from 11 Mbps to 5.5 Mbps as range increases or signal quality decreases. Subsequent fallbacks from 5.5 Mbps to 2 Mbps and 1 Mbps are also supported.

Interference and Coexistence

802.11 operates in a range of radio frequencies known as an "unlicensed" band (i.e., the FCC does NOT require the use of a license in order to operate a radio transmitter in this range). This means that commercially available radio devices other than wireless LAN devices are permitted to use the same frequency band as 802.11. Consequently, these co-existing radio devices can interfere or "jam" the wireless LAN (and vice versa). The most troublesome devices are cordless telephones and microwave ovens.

Fortunately, higher quality cordless phones tend to "listen" for a clear channel before becoming active and will thus avoid interfering with a wireless LAN (i.e., the cordless phone seeks a clear channel for itself so naturally avoids being interfered with or being a source of interference). Jamming from microwave ovens is more severe but is usually restricted to the upper frequency range for 802.11 (it should be noted that 802.11b/g divides the available frequency band into 11 channels (US). The higher numbered channels are most susceptible to microwave oven interference).

In each instance, jamming occurs only when the cordless telephone or microwave oven is active.

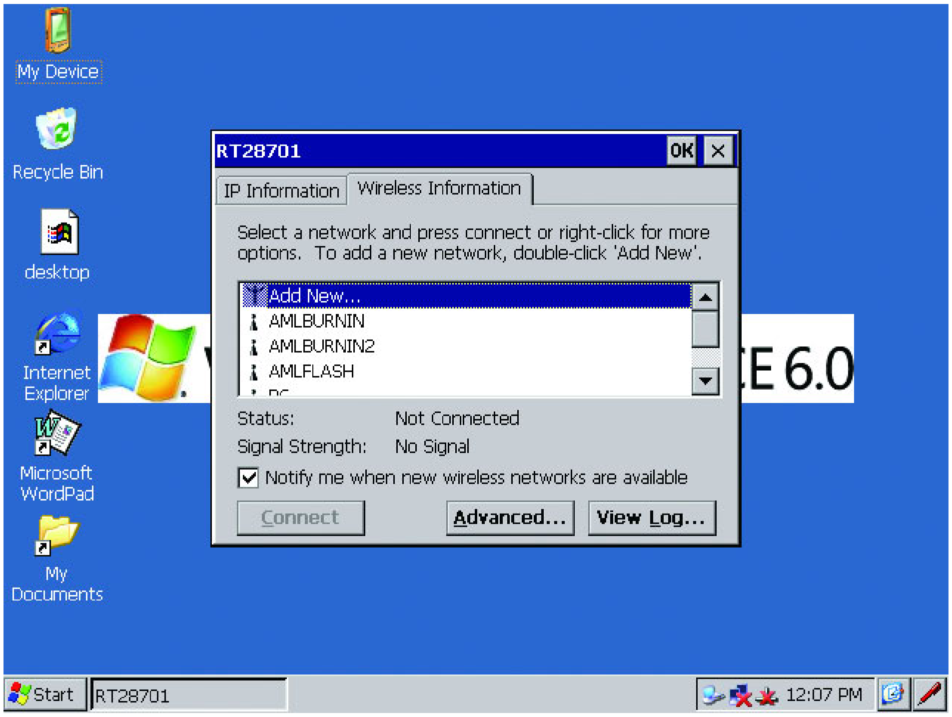
Encryption and Authorization

Much has been publicized in the mass media recently about security problems with wireless LANs. Although it cannot be denied that some encryption algorithms currently used in 802.11 are flawed, the fact is that security breaches of a wireless LAN require a deliberate attempt to access the network by an intruder.

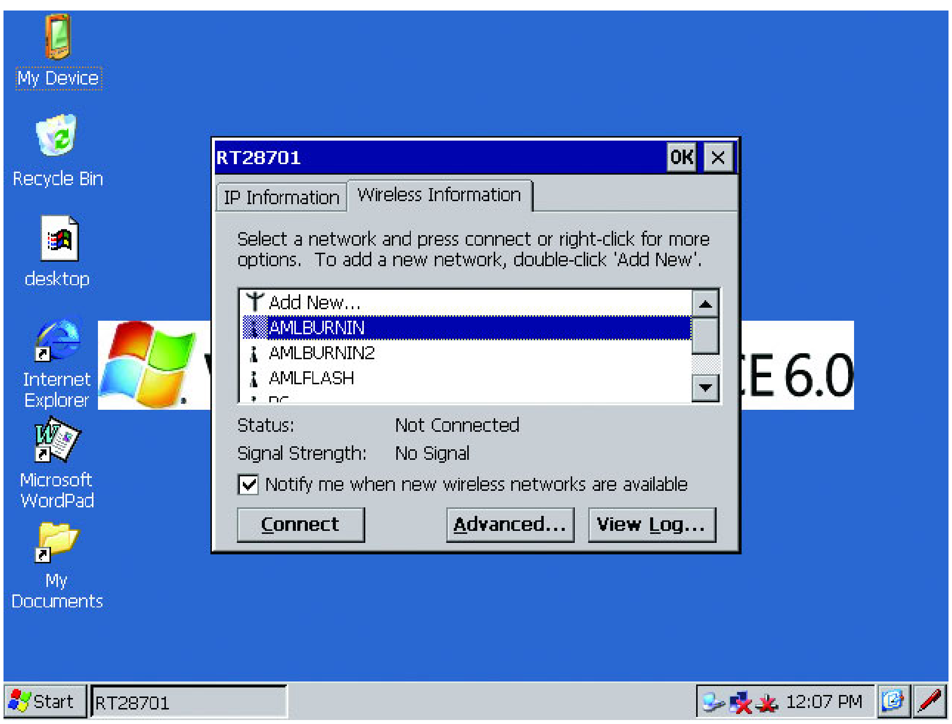
The primary issue is that many current users of wireless LAN have opted NOT to turn on security features. If users were to enable the security features currently available (including only allowing known systems access to the network and enabling WEP (Wired Equivalent Privacy) or WPA (Wifi Protected Access)) on even the most basic access points, the intruder's work is much harder. Much as a burglar will stray away from a house whose doors and windows are securely locked, so too will an attacker tend to move past a wireless network when even the simplest security measures are enabled.

Wireless Configuration

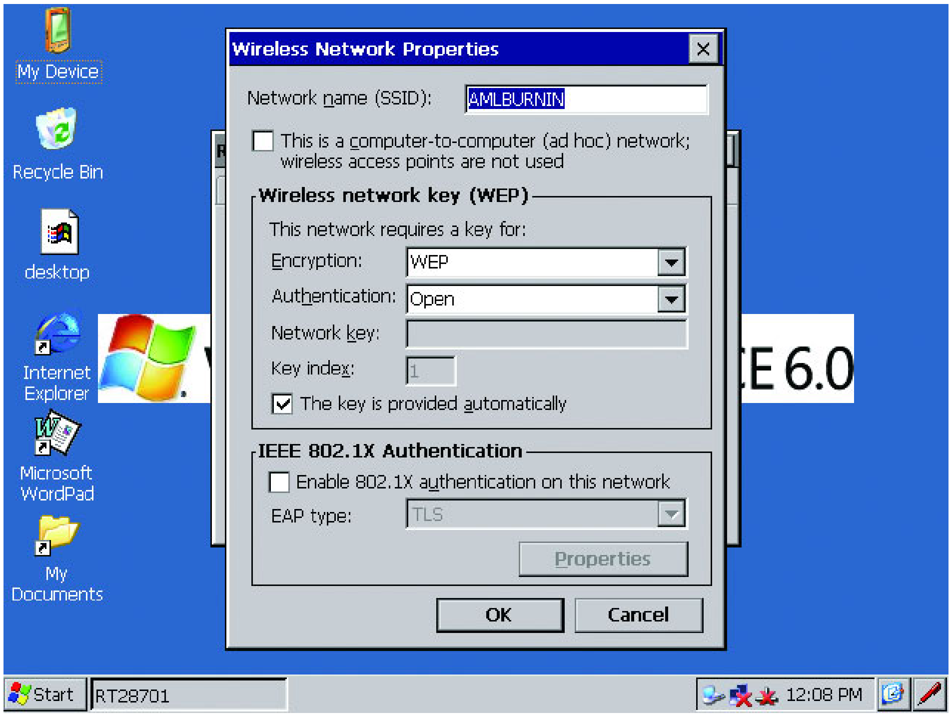
The optional 802.11b/g/n radio can be configured with the KDT900 Setup Utility under the Windows Wireless setup screens.



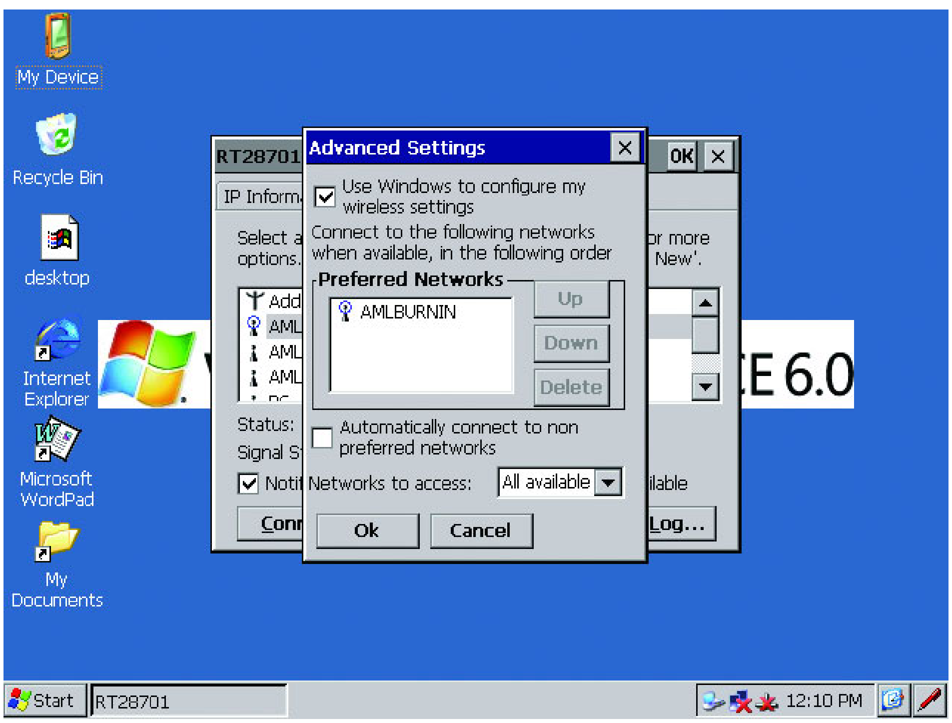
If the KDT900 has the optional Wireless radio, the unit will boot into the Windows Wireless setup menu. The unit will automatically search for available wireless networks.



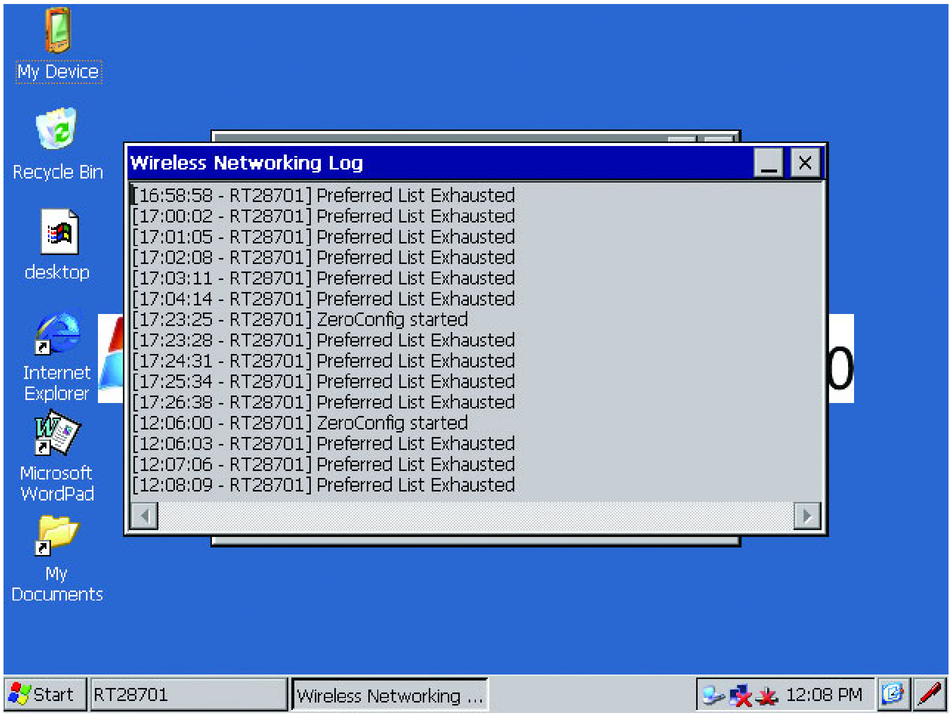
Use the KDT900 touch screen to select the wireless network you want to connect to. Note the unit is “Not Connected” under Status.



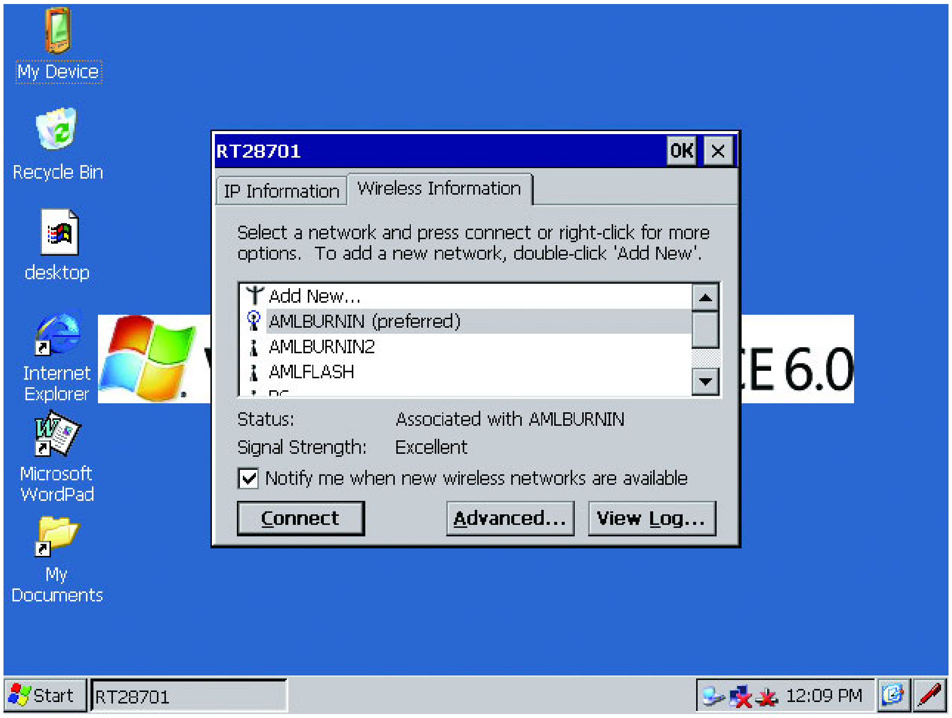
Many wireless networks require the proper passwords or network keys to connect. Contact your systems administrator to find out the proper network and password or keys.



Once you have selected a proper wireless network, you can control the order by which the KDT900 will attach under Advanced Settings.



You can view the Wireless Network Log in order to see what the KDT900 is doing.



Once you are connected to a wireless network the Status will change and the Signal Strength will be displayed.

6

Integrated Bar Code Scanner

This chapter describes the use of the internal bar code reader.

Overview

The KDT900 terminals can contain an integrated or externally-mounted bar code reader for decoding bar code symbols in a variety of formats.

The terminal can be equipped with a linear CCD imager a 1D laser, a 2-Dimensional, omni-directional imager, an externally-mounted, omni-directional laser, or no bar code scan engine at all.

It is important to know what type of engine is installed in the unit to allow for correct customization of the engine.

Determining Scanner Type

The type of scanner can be determined either by the KDT900's model number reference chart at the beginning of this document or by observing the scanner's decode pattern.

If the KDT900 model number ends in a zero, the unit contains no internal scan engine:
KDT900-xxx0

If the KDT900 model number ends in a one, the unit contains the Linear CCD engine:
KDT900-xxx1

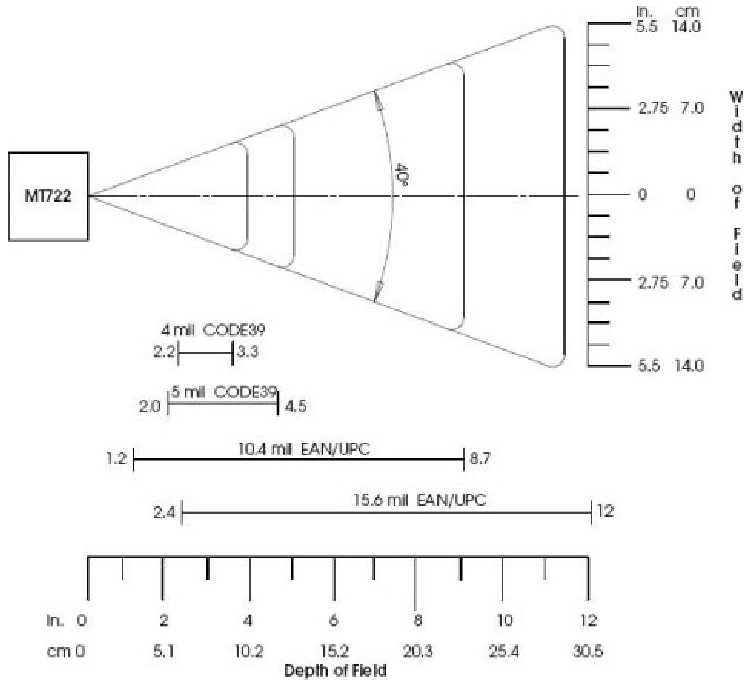
If the KDT900 model number ends in a two, the unit contains the 2D Omni-directional engine:
KDT900-xxx2

If the KDT900 model number ends in a three, the unit contains the 1D Laser engine:
KDT900-xxx3

If the KDT900 model number ends in a four, the unit contains the External Omni-directional engine:
KDT900-xxx4

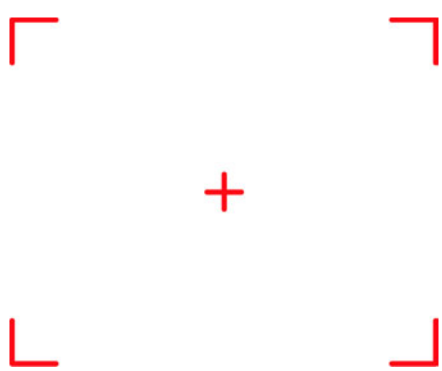
Linear CCD Decode Zones

The Linear CCD can only read symbols that are within its field of view:



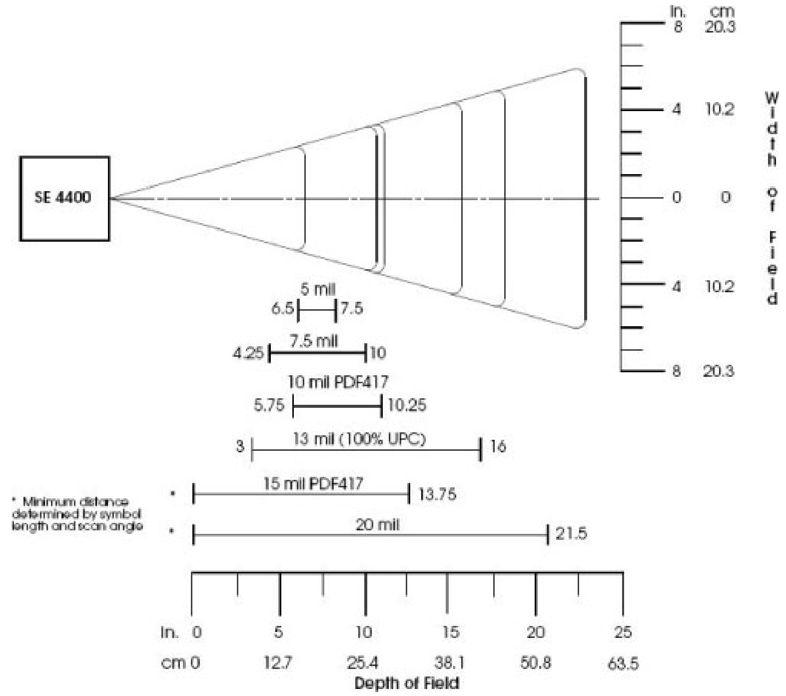
2D Omni Scanner Aiming System and Decode Zones

The 2D Omni-directional scanner will use a 650nm laser to draw an aiming pattern of the decoder's decode zone:

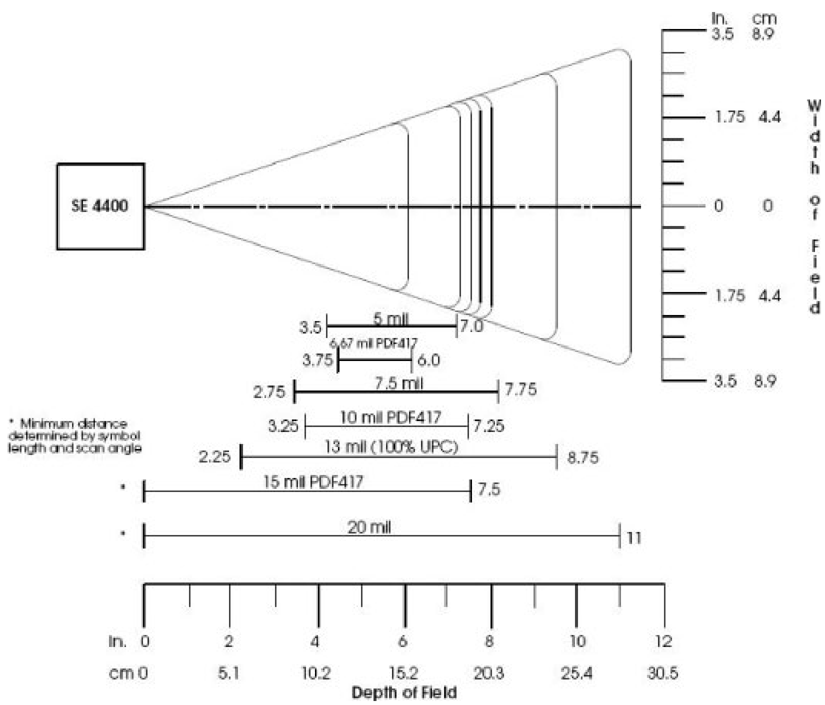


The decoder is only capable of decoding symbols that are within its field of view. Two focus modes are selectable for the 2D imager:

Far Focus:



Near Focus:



Triggering

The KDT900's internal bar code scanners are designed to be used in presentation modes. In these modes, the scanner is always scanning and looking for bar codes to decode.

NOTE: Some internal scanners have the ability to disable the illumination LEDs when no bar code is present under the scanner. The scanner is still looking for bar codes, but is saving power by only enabling the illumination when a new bar code symbol is present.

To manually trigger the bar code decoder, use the *Data Viewe*r tool under the *System Tools* folder.

Scanning Bar Codes

NOTE: Bar codes will only be scanned when software that is aware of the bar code interface is running.

Scanning with the Linear CCD

KDT900 units equipped with the Linear CCD scan engine require proper alignment of the bar code under the scanner window. The Linear CCD's ideal scanning range is between 2.5 inches and 8 inches.

Scanning with the Omni-Directional Imager

The 2D Omni-directional imager is capable of scanning bar codes at any orientation as long as the entire symbol is visible to the scanner and illuminated.

Supported Symbologies

Symbology	Linear CCD	2D Imager
UPC/EAN	X	X
Code 39	X	X
Code 93	X	X
Code 128	X	X
Interleaved 2 of 5	X	X
Discrete 2 of 5	X	X
MSI/Plessy	X	X
Codabar	X	X
Code 11	X	X
GS1 (Formerly RSS)	X	X
Postal Codes	(Chinese Only)	X
Composite Codes		X
PDF417		X
MicroPDF417		X
Maxicode		X
Data Matrix		X
QR Code		X

Obtaining and Using Setup Bar Codes

The internal bar code scanners can be configured with special setup bar code symbols. These symbols are specific to the model of bar code scanner installed in the unit and are available from AML.

The default parameters and trigger mode bar codes are listed below.

NOTE: The unit will NOT make an audible beep after scanning a setup bar code.

Parameter	Linear CCD	2D Omni-directional Imager
Set All Defaults	Parameters Default	Parameters Default
Set Decode Mode	Continuous Decoding (Always On)	Continuous Decoding (Always On)
Set Focus	N/A	Focus Near Focus Far Smart Focus (Alternate between near and far)

7

Windows® Embedded CE 6.0

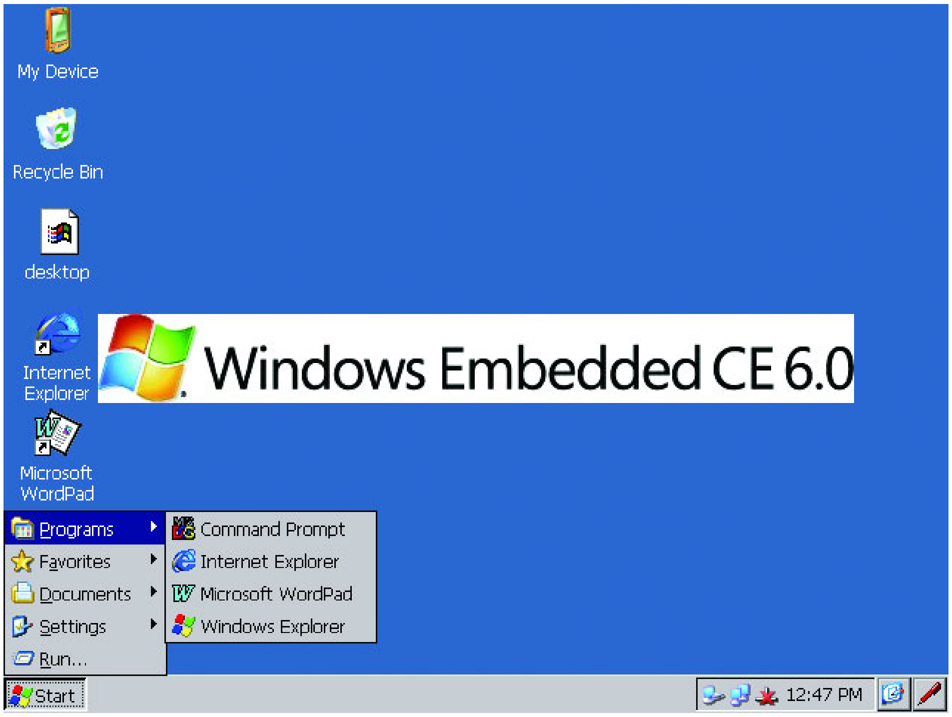
This chapter describes the Windows® Embedded CE 6.0 software on the KDT900.

Windows® Embedded CE 6.0

The KDT900 unit is preloaded with Windows® Embedded CE 6.0 Professional from Microsoft.

General Usage

Windows® Embedded CE 6.0 works much like other Microsoft® operating systems. The desktop is arranged with the standard taskbar, icons, and Start button that exists in all versions of Windows.

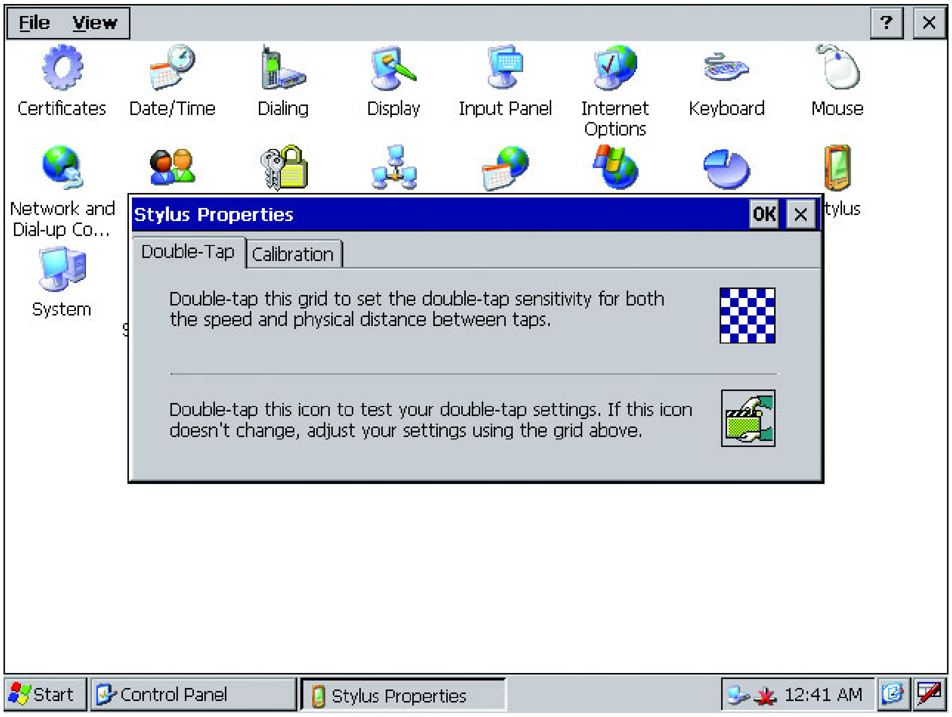


Tapping the touchscreen emulates a left mouse click in the desired area, and holding down a stylus or finger in one location will create a right mouse click.

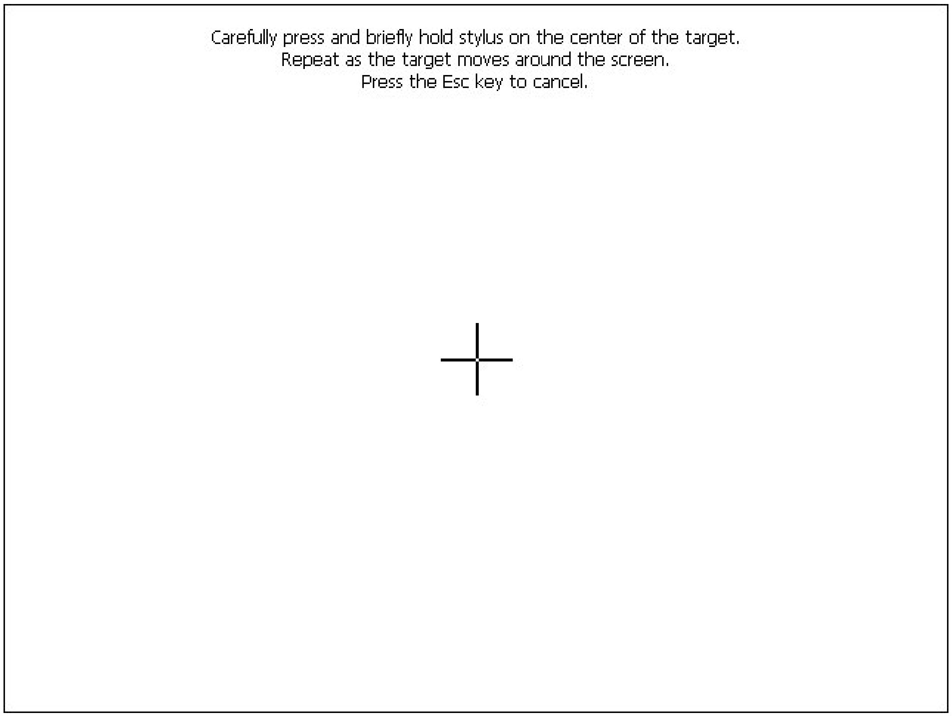
Calibrating the Touchscreen

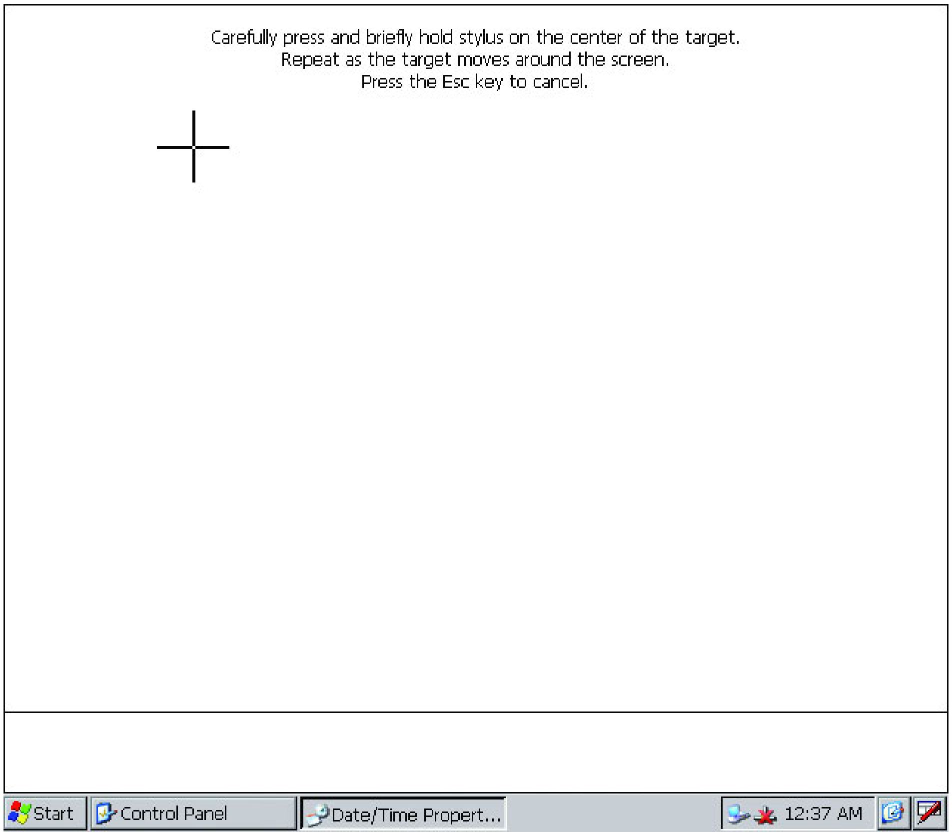
Environmental conditions such as temperature can cause the touchscreen and LCD alignment to drift. Recalibrating the touchscreen will align the two devices.

To calibrate the touchscreen, select the **Stylus** application from the **Control Panel**, and begin the calibration procedure from the **Calibration** tab.



Calibration is completed by holding the stylus on the screen at the indicated target. The process will repeat until a valid calibration sequence is completed and the target disappears.

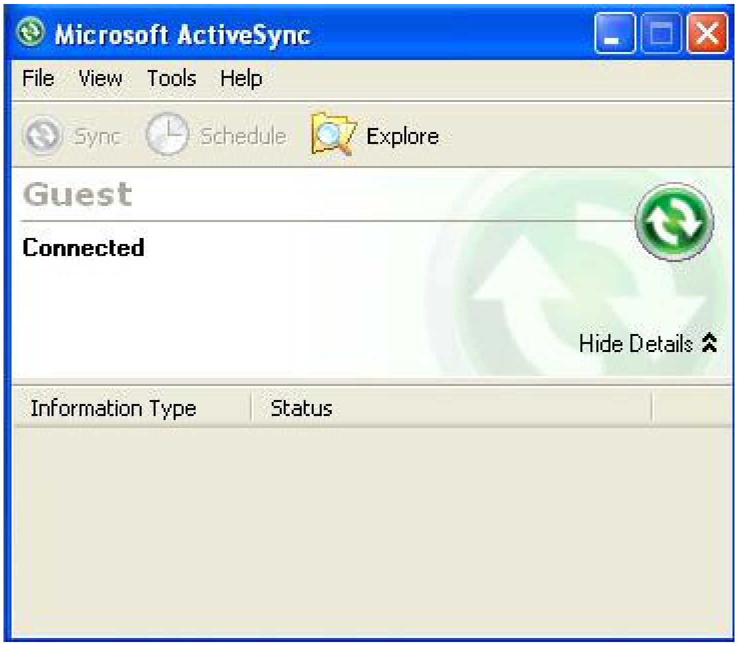




Connecting to a PC

The KDT900 communicates via USB to a PC running any modern version of the Microsoft Windows® operating system. The host PC must have either Microsoft ActiveSync® or Microsoft Windows® Mobile Device Center installed and configured properly to communicate with the KDT900. These applications are available for free from Microsoft.
To connect, make sure the KDT900 is fully powered on and the operating system has booted completely. Plug in the USB cable from the KDT900 to an available USB port on the PC.

See *Chapter 4* for information on cable requirements for ActiveSync® connections.

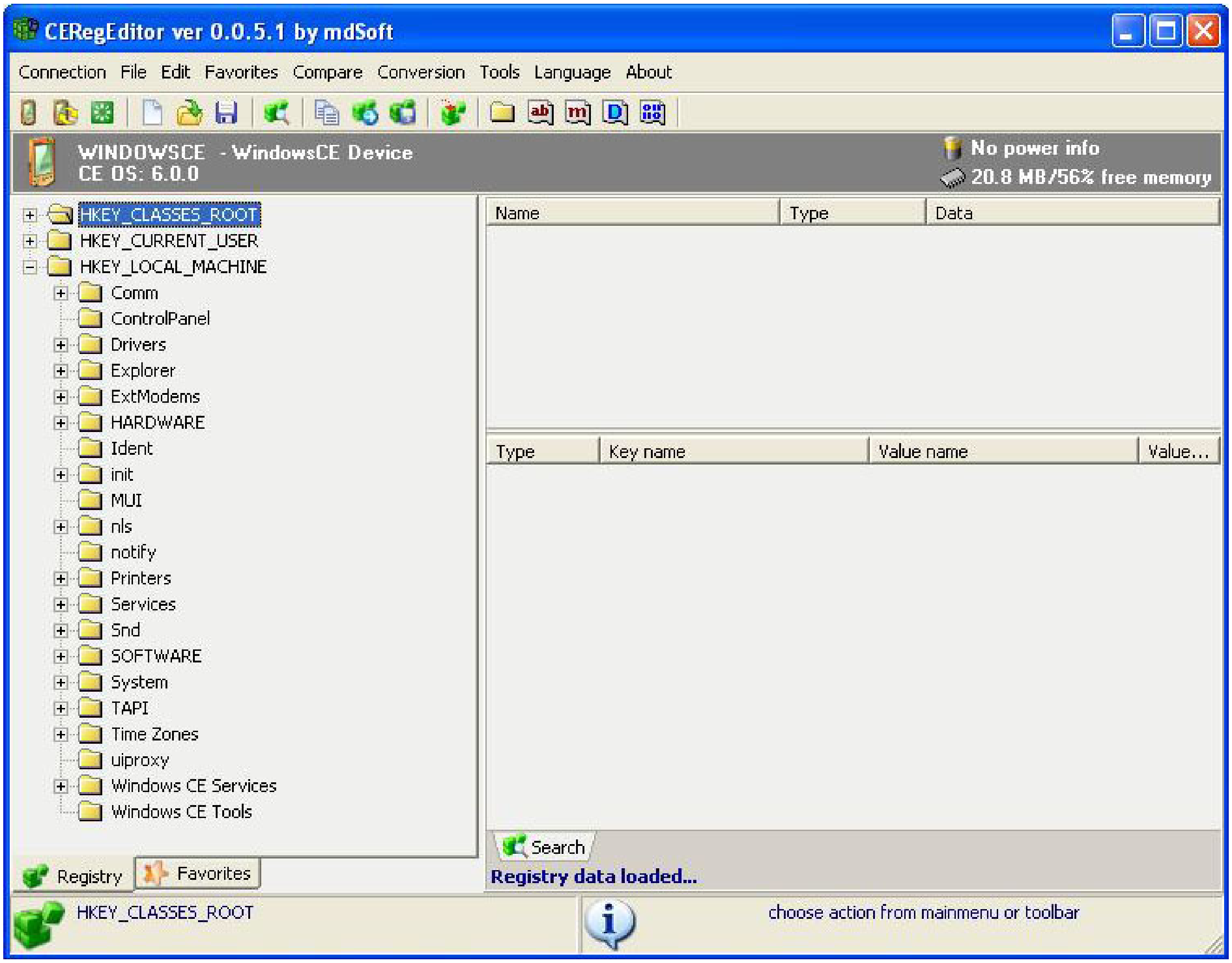


ActiveSync® will automatically create the connection and allow browsing from the PC to the device filesystem. Files can be copied to and from the KDT900 with Windows® Explorer.

Programming the Pushbuttons

The four pushbuttons on the KDT900 can be configured to any standard key on a PC keyboard. By default, these keys are, from left to right, the Windows (Start Button) key, Up Arrow, Down Arrow, and Enter.

Changing the keys requires an ActiveSync® connection as described above and a Remote Registry Editor. AML recommends **CERegEditor** by **mdSoft** for editing the registry keys via ActiveSync®.



Connect the KDT900 to the PC via ActiveSync® and start the registry editor. To change the keys, edit the following registry keys as described:

HKLM/Drivers/AML/Pushbuttons		
ButtonA	DWORD	ASCII equivalent of the desired keystroke that corresponds to the given pushbutton.
ButtonB	DWORD	
ButtonC	DWORD	
ButtonD	DWORD	

Non-ASCII codes:

0x01 - Left	0x02 - Right	0x03 – Up
0x04 - Down	0x05 – Start Menu	0x80 – F1
0x81 – F2	0x82 – F3	0x83 – F4
0x84 – F5	0x85 – F6	0x86 – F7
0x87 – F8	0x88 – F9	0x89 – F10
0x8a – F11	0x8b – F12	0x8c – F13
0x8d – F14	0x8e – F15	0x8f – F16
0x90 – F17	0x91 – F18	0x92 – F19
0x93 – F20	0x94 – F21	0x95 – F22
0x96 – F23	0x97 – F24	

Changing the MSR and Barcode Reader Settings

The Magnetic Stripe Reader and Barcode Scanner settings can be changed via the same method as the Pushbuttons described above. The following keys are valid for the MSR and barcode reader:

HKLM/Drivers/AML/Barcode		
Enable	DWORD	Set to 1 to enable barcode reading; set to 0 to disable *NOTE: The scanner will always appear on*
KeyboardWedge	DWORD	Set to 1 to present the data as keyboard input
StripSpaces	DWORD	Set to 1 to strip spaces in the barcode data
TermCharacter	DWORD	Append this ASCII character to the end of the barcode

HKLM/Drivers/AML/Magstripe		
Enable	DWORD	Set to 1 to enable reading data from the MSR; set to 0 to disable *NOTE: The MSR will always be powered on*
KeyboardWedge	DWORD	Set to 1 to present the data as keyboard input
StripSpaces	DWORD	Set to 1 to strip spaces in the barcode data
TermCharacter	DWORD	Append this ASCII character to the end of the barcode

Persistent Storage

The entire filesystem of the KDT900 will persist between cold boots. Files and settings that need to be retained can be written to any location of the root filesystem or onto the Storage Card mount.

The KDT900 includes an internal 1 GB (1024MB) Secure Digital (SD) card mounted under “Storage Card” in the root filesystem. This card contains the Windows® Embedded CE operating system firmware. The firmware is stored as a normal file with the name “KDT900.k9x” in the root directory of the SD card. DO NOT DELETE THIS FILE.

NOTE: The SD card must be present for the KDT900 to operate.

NOTE: A proper Windows® Embedded CE 6.0 firmware image must be in the root directory of the SD card for the KDT900 to boot.

Free space (~1000MB) on the SD card can be used for data storage, program installation, or other custom applications, however, the SD card is much slower compared to the internal flash memory (root filesystem). It is recommended that if the internal flash is large enough to house the custom application or data, it should be used in preference over the SD card.

Preinstalled Software

The Windows® Embedded CE 6.0 operating system has been configured with a number of applications and packages including:

- WordPad
- Pocket Internet Explorer®
- .NET Compact Framework 2.0
- CAB File Installer/Uninstaller
- ActiveSync®
- ATL & COM
- Command Processor and Console

A complete list of Windows® Embedded CE components available in the base firmware can be obtained from AML. To request additional Windows® Embedded CE components, contact the AML support staff.

8

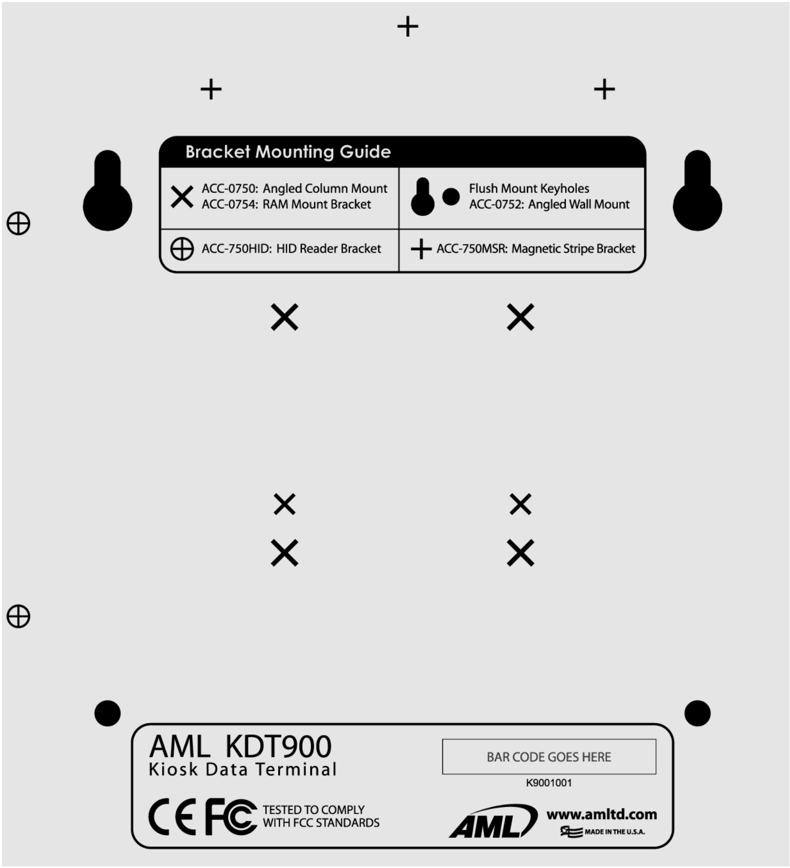
Mechanical Integration and Mounting

This chapter describes methods to mount the KDT900 unit in a variety of environments.

Rear Panel Mount Points

The KDT900 base unit is backed by a stainless steel rear panel with a variety of mounting patterns. Each pattern is indicated by the rear label. A sharp punch or knife can be used to punch through the label at the desired locations, and only the necessary holes should be knocked out to keep the unit environmentally sealed.

WARNING: THE REAR PANEL SHOULD BE REMOVED FROM THE OUTER CASE BEFORE PUNCHING ANY HOLES IN THE LABEL.

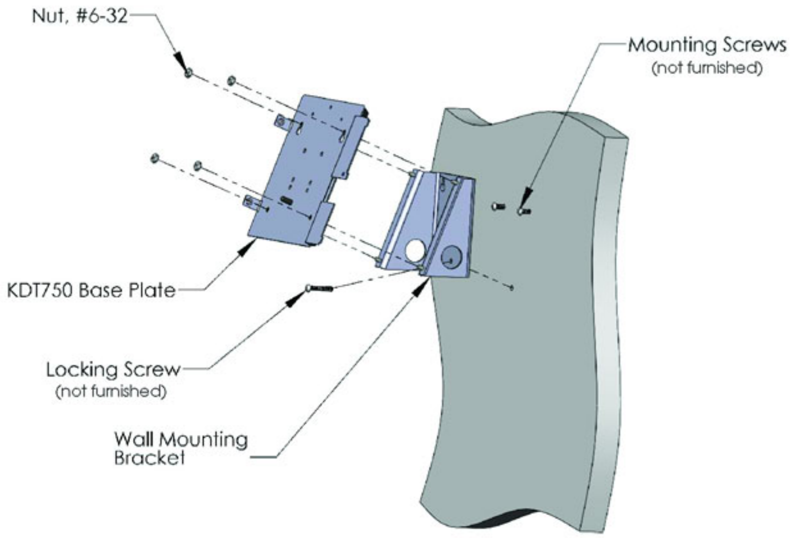


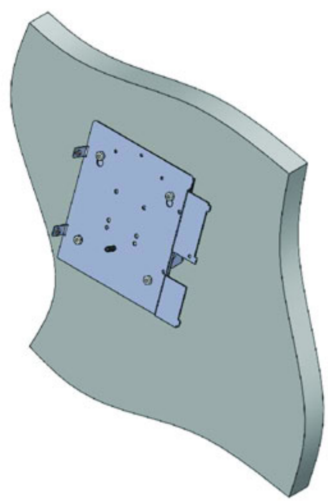
Flush Wall Mounting

The KDT900 base unit can be flush mounted with four screws via four holes in the rear panel (two "key-hole", two round). The rear panel's cable inlet is recessed, allowing for flush mounting in certain situations.

Angled Wall Mounting

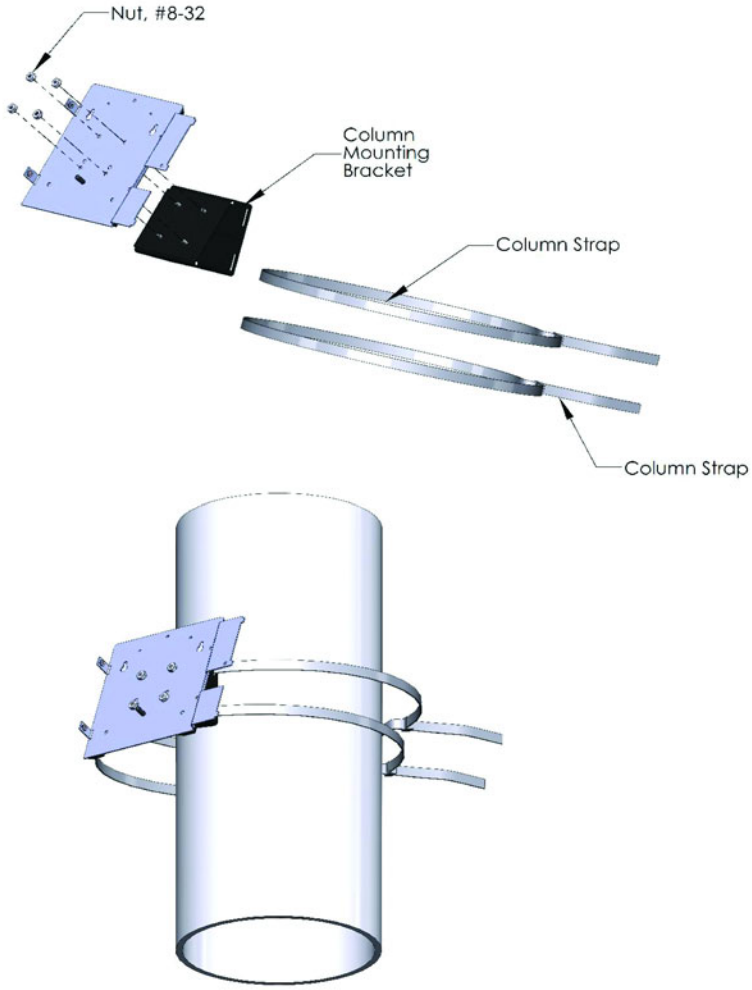
The optional Angled Wall Bracket (ACC-0752) hard mounts the KDT900 to any flat surface at a 20 degree angle, ideal for price checking applications. The bracket attaches to the KDT900's rear panel via four stainless steel studs and nuts.





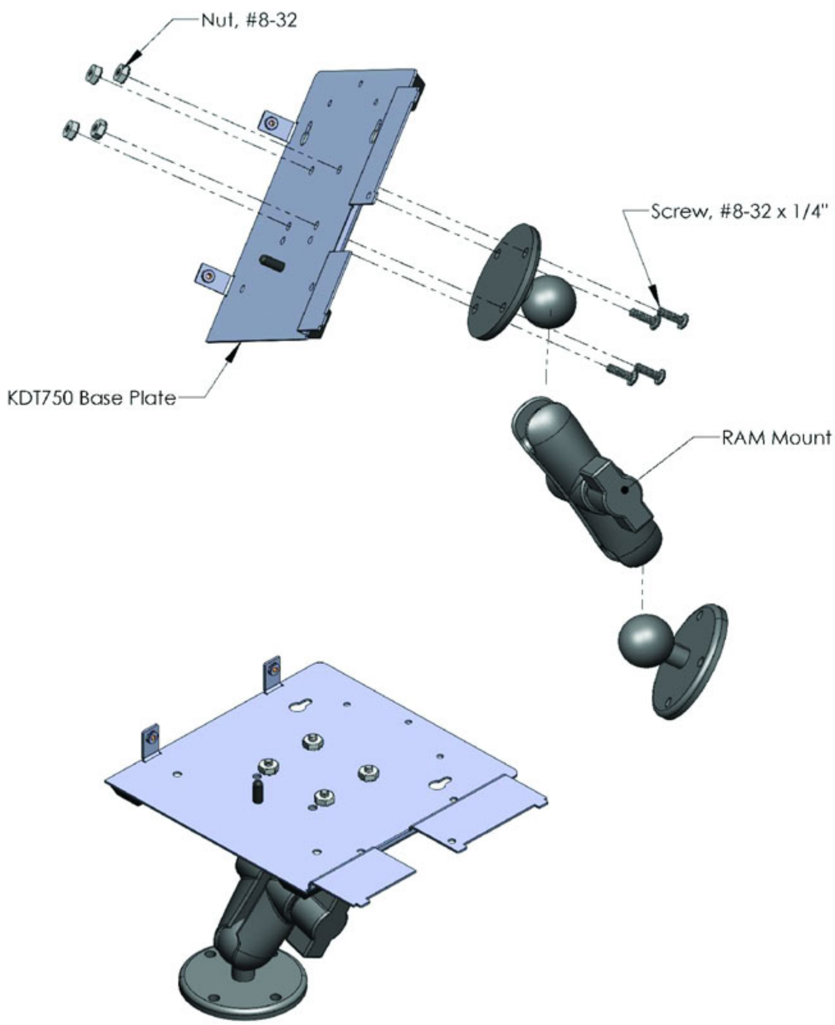
Column/Post Mounting

The KDT900 Pole Mount bracket (ACC-0750) is a non-destructive mounting solution for existing round structural or aesthetic posts and poles. By utilizing nylon or steel straps, the unit can be mounted to poles ranging in sizes from 4 to 24 inches in diameter. The ideal pole diameter for the bracket ranges from 6 to 16 inches.



RAM Mounts

The KDT900 can be mounted with the standard "B" size RAM® Mounting system. The rear panel of the base unit houses the standard 4 hole AMPS bolt pattern for attaching RAM ball and socket mounts. The RAM mounting system includes fully adjustable mounts, as well as locks, bases, accessory mounts and extensions.



Appendix A

Technical Specifications

General Specifications	
Dimensions	14.6 cm L x 7.2 cm W x 5.0 cm D(5.750" L x 6.625" W x 2.000" D)
Weight	0.81 lbs./363g
Display	5.6" VGA (640x480), 16-bit Color TFT LCD
Touchscreen	Integrated Resistive Touch Panel
Keypad	4 x Integrated momentary push-button
Power Supply	Power-over-Ethernet (48V, 802.3af Compliant) 12V DC 2.1 mm Barrel Jack
Internal UPS Battery	7.4V 2-Cell 2200 mAh Lithium-ion, ~1 hour runtime (Optional)
I/O Ports	3 x USB 1.1 Full Speed Host Ports 2 x RS-232 (1 x RJ-45, 1 x Expansion Header) 1 x Wiegand Interface (Header) 2 x Isolated Digital Inputs (Screw Terminal Block) 2 x Isolated Micro-Relay Outputs (Screw Terminal Block) 2 x Internal Bar Code Decoder Connector (12 & 14 Pin FPC Flex)
Networking	10/100Base-TX Fast Ethernet 802.11b/g/n Wireless Radio (Optional Internal USB Type)
Audio	Integrated Speaker and Amplifier (tonal)
Bar Code Decoding	Integrated Linear CCD Imager (Optional) Integrated Omni-Directional, 2D Imager (Optional) Integrated 1D Laser (Optional) External Omni-Directional Laser (Optional)
Card Reading	Magnetic Stripe Reader (Optional) HID® ProxPoint® Proximity Card Reader (Optional)

Performance Specifications	
Processor	Samsung S3C2410 @ 202 MHz
Architecture	32-bit RISC ARM9 with AMBA (Advanced Microcontroller BusArchitecture)
Memory (RAM)	64 MB 100MHz SDRAM
Memory (Flash storage)	1024 MB (1 GB) Storage (SD Card) 16 MB Integrated Flash ROM (Operating System)
Memory Expansion	1 GB SD Card Included
Operating System	Windows® Embedded CE 6.0

Environmental Specifications	
Operating Temperature	-20° to 50° C / -4° to 122° F
Storage Temperature	-30° to 60° C / -30° to 140° F
Humidity	0% to 90% RH, non-condensing
Electrostatic Discharge	15kVDC through air 8kVDC contact
Sealing	IP54 NEMA 12

Regulatory Specifications	
Certifications	FCC, CE
Environmental	RoHS, Pb-Free

Optional Wireless Radio Specifications	
Radio	IEEE 802.11n Draft v2.0; IEEE 802.11b; IEEE 802.11g
Frequency	2.4 GHz Range
Signal Rates	11n (40MHz): up to 300Mbps; 11n (20MHz): up to 144Mbps; 11g: up to 54Mbps; 11b: up to 11Mbps
Output Power	802.11b: 17± 1dBm 802.11g: 17± 1dBm 802.11n: 15± 1dBm
Antenna Configuration	1T2R Internal Antenna (1 Transmit / 2 Receiving)
Receive Sensitivity	802.11g: -70dBm @54Mbps 802.11b: -83dBm @11Mbps 802.11n: -83dBm @11Mbps
Security	None 64/128 Bit WEP WPA/WPA2 Personal (PSK) WPA/WPA2 Enterprise (EAP) 802.1x Authentication Supplicants

Appendix B

Wireless Reference Table

Wireless Reference Table		
WEP	Remote Authentication Dial In User Service	WEP was initially intended to provide a level of confidentiality on a wireless network that was comparable to a wired infrastructure. WEP does not allow for any true authorization (only encryption) and does not protect users or devices from each other on the network. There are two main WEP types: WEP Open System (Standard WEP) – All data transmissions are encrypted with the WEP key. No attempt is made to authorize the client device. WEP Shared Key – In Shared Key, a very insecure attempt to authorize the device is attempted. The actual WEP encryption key is sent to the host (usually the access point) to verify the identity of the device. This exposes the enciphering key to the network, and should not be used. In a WEP enabled environment, each client holds the common network encryption keys which can be either a 40-bit key for 64-bit encryption or a 104-bit key for 128-bit encryption. These keys are common to all devices on the network and are used to encrypt all data transmissions. Because each network packet is encrypted with the same key, and because of flaws in the actual cipher, WEP is no longer considered secure, and an attacker, depending on network traffic, could determine the network encryption keys by eavesdropping on the transmissions. It has been demonstrated in a controlled environment that these attacks can take as little as 10 minutes to determine a 40-bit key.
WPA	Wifi Protected Access	WPA was created in response to the weaknesses of WEP, and while it implements the majority of the IEEE 802.11i standard, it is not considered to be fully compliant. WPA was only intended as a temporary measure to be used in place of WEP while the final 802.11i standard was being drafted. WPA was designed to work on all existing 802.11 hardware to provide a considerable amount of protection compared to WEP. WPA was designed for use with an 802.1x (commonly referred to as RADIUS) server to provide authentication and to distribute encryption keys to the clients. It is possible, however, to use WPA in "Personal" Pre-shared key (PSK) mode which allows the benefits of WPA without the need of the external 802.1x server, but this is

Wireless Reference Table

		considered to be less secure. Each client in a PSK environment holds a common passphrase that is used to generate the keys. Weak passphrases is the major concern when using PSK. One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used. The more often that the encryption key changes, the less data a potential attacker can get on the key, and, even if they were to determine the current key, once a new key was rotated in, they would de-authenticated again. WPA also defined the use of EAP for authentication of users, however it does not define all of the EAP types that are employed in WPA2.
WPA2	Wifi Protected Access Version 2	WPA2 contains the following components: 802.1x for authentication (entailing the use of EAP and an authentication server), RSN (Robust Security Network) for keeping track of associations, and AES-based CCMP encryption to provide confidentiality, integrity and origin authentication. The CCMP algorithm is the heart of WPA2 and is what sets it apart from WPA. CCMP was designed to replace both TKIP and WEP, and handles message integrity, encryption and authentication. Most, if not all of the capabilities of WPA can be implemented in WPA2 with CCMP, which is considered the state of the art.
802.11i	IEEE 802.11i Standard	The IEEE standard. Commonly called WPA2.
TKIP	Temporal Key Integrity Protocol	Dynamic key rotation algorithm often used in WPA environments.
CCMP (AES)	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol	Encipherment algorithm designed to replace TKIP and WEP in WPA2/802.11i. CCMP is considered state of the art.
EAP	Extensible Authentication Protocol	EAP is a general authentication method that can be used in many technologies, but it is most commonly found in wireless LANs. A large amount of documentation refers to WPA-EAP as "WPA Enterprise" even though it is an ambiguous term. There are many subtypes of EAP, but only five have been described as standard. The MT7570 supports the following EAP types for authentication. EAP-TLS – EAP Transport Layer Security is the original standard wireless LAN EAP authentication protocol. Although it is rarely deployed, it is still considered one of the most secure EAP standards available and

Wireless Reference Table		
		the most secure EAP standards available and is universally supported by all manufacturers of wireless LAN hardware and software. The requirement for a client-side certificate, however unpopular it may be, is what gives EAP-TLS its authentication strength and illustrates the classic convenience vs. security trade-off. EAP-TTLS - Tunneled Transport Layer Security was co-developed by Funk Software and Certicom and is widely supported across platforms. It was never fully ratified, only drafted (the draft which has since expired), but is still common due to its decent level of security and easy setup. EAP-PEAP - Protected Extensible Authentication Protocol is widely available in products, and provides very decent authentication security. Its method is similar in design to EAP-TTLS but requires only a server-side certificate to create a secure tunnel to protect user authentication. PEAPv0/EAP-MSCHAPv2 is what most are referring to when the term "PEAP" is used. Behind EAP-TLS, PEAPv0/EAP-MSCHAPv2 is the second most widely supported EAP standard in the world. EAP-LEAP - The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary EAP method developed by Cisco Systems, Inc. It is considered less secure than other EAP types, even by Cisco, and is not recommended in new installations.
PSK	Pre-shared Key	Often called "WPA/WPA2 Personal", PSK allows the use of common passphrases for authentication. PSK is often used in smaller networks that wish to use the high security of WPA/WPA2 but do not wish to employ an 802.1x authentication server.
802.1x	IEEE 802.1X	IEEE Standard for authentication. Often in wireless documentation, references to"802.1x" are really meaning 802.1x Authentication Server or RADIUS server that provides authentication and encryp-tion keys to the clients.
RADIUS	Remote Authentication Dial In User Service	Often, administrators will call the 802.1x server the "RADIUS" server. RADIUS is an authentication, authorization, and accounting protocol for applications such as network access or IP mobility. In the wireless LAN environment, RADIUS is commonly used to implement the 802.1x standard.